

# BRAUER RELATIONS IN FINITE GROUPS

ALEX BARTEL<sup>1</sup> AND TIM DOKCHITSER<sup>2</sup>

ABSTRACT. If  $G$  is a non-cyclic finite group, non-isomorphic  $G$ -sets  $X, Y$  may give rise to isomorphic permutation representations  $\mathbb{C}[X] \cong \mathbb{C}[Y]$ . Equivalently, the map from the Burnside ring to the rational representation ring of  $G$  has a kernel. Its elements are called Brauer relations, and the purpose of this paper is to classify them in all finite groups, extending the Tornehave-Bouc classification in the case of  $p$ -groups.

## CONTENTS

1. Introduction	2
1.1. Background and main result	2
1.2. Overview of the proof	4
1.3. Remarks and applications	4
1.4. Notation	6
2. First properties	7
3. Imprimitivity criteria	8
4. A characterisation in terms of quotients	11
5. Primitive relations in $p$ -groups	12
6. Main reduction in soluble groups	13
7. Quasi-elementary groups	18
7.1. The kernel of the conjugation action	18
7.2. A generating set of relations	21
7.3. Primitive relations with trivial $K$	24
7.4. Primitive relations with non-trivial $K$	27
8. Examples	31
9. An application to regulator constants	32
References	34

---

<sup>1</sup>MATHEMATICS INSTITUTE, ZEEMAN BUILDING, UNIVERSITY OF WARWICK, COVENTRY CV4 7AL, UK

<sup>2</sup>DEPARTMENT OF MATHEMATICS, UNIVERSITY WALK, BRISTOL BS8 1TW, UK  
*E-mail addresses:* [a.bartel@warwick.ac.uk](mailto:a.bartel@warwick.ac.uk), [tim.dokchitser@bristol.ac.uk](mailto:tim.dokchitser@bristol.ac.uk).  
2000 *Mathematics Subject Classification.* 19A22, 20B05, 20B10.

## 1. INTRODUCTION

**1.1. Background and main result.** The Burnside ring  $B(G)$  of a finite group  $G$  is the free abelian group on isomorphism classes of finite  $G$ -sets modulo the relations  $[X] + [Y] = [X \amalg Y]$  and with multiplication  $[X] \cdot [Y] = [X \times Y]$ . There is a natural ring homomorphism from the Burnside ring to the rational representation ring of  $G$ ,

$$B(G) \longrightarrow R_{\mathbb{Q}}(G), \quad X \mapsto \mathbb{Q}[X].$$

The purpose of this paper is to describe its kernel.

Both the kernel and the cokernel have been studied extensively. The cokernel is finite of exponent dividing  $|G|$  by Artin's induction theorem, and Serre remarked that it need not be trivial ([28] Exc. 13.4). It is trivial for  $p$ -groups [19, 26, 27] and it has been determined in many special cases [18, 8, 22].

Elements of the kernel  $K(G)$  are called *Brauer relations* or *( $G$ -)relations*. The most general result on  $K(G)$  is due to Tornehave [31] (see [23, 2.4]) and Bouc [11], who independently described it for  $p$ -groups.

There is a bijection  $H \mapsto G/H$  between conjugacy classes of subgroups of  $G$  and isomorphism classes of transitive  $G$ -sets, and we will write elements  $\Theta \in B(G)$  as  $\Theta = \sum_i n_i H_i$  using this identification. In this notation,

$$\Theta \in K(G) \iff \sum_i n_i \operatorname{Ind}_{H_i}^G \mathbf{1}_{H_i} = 0.$$

If we allow inductions of arbitrary 1-dimensional representations instead of just the trivial character, isomorphisms between sums of such inductions are called monomial relations. Deligne [13, §1] described all monomial relations in soluble groups, following Langlands [25]. For arbitrary finite groups, a generating set of monomial relations was given by Snaith [30].

Following the approach of Langlands, Deligne, Tornehave and Bouc, we consider a relation “uninteresting” if it is induced from a proper subgroup or lifted from a proper quotient of  $G$  (see §2). We call a relation *imprimitive* if it is a linear combination of such relations from proper subquotients and *primitive* otherwise, and we let  $\operatorname{Prim}(G)$  denote the quotient of  $K(G)$  by the subgroup of imprimitive relations. The motivation for this approach is that if one wants to prove a statement that holds for all Brauer relations, and if this statement behaves well under induction and inflation, then it is enough to prove it for primitive relations (see also §1.3).

In this paper we classify finite groups that have primitive relations and determine  $\operatorname{Prim}(G)$ :

**Theorem A.** *Let  $p$  denote a prime number. A finite non-cyclic group  $G$  has a primitive relation if and only if either*

- (1)  $G$  is dihedral of order  $2^n \geq 8$ ; or
- (2)  $G = (C_p \times C_p) \rtimes C_p$  is the Heisenberg group of order  $p^3$  with  $p \geq 3$ ; or
- (3)  $G$  is an extension

$$1 \longrightarrow S^d \longrightarrow G \longrightarrow Q \longrightarrow 1,$$

where  $S$  is simple,  $Q$  is quasi-elementary, the natural map  $Q \rightarrow \text{Out } S^d$  is injective and, moreover, either

- (a)  $S^d$  is minimal among the normal subgroups of  $G$   
(for soluble  $G$ , this is equivalent to  $G \cong \mathbb{F}_l^d \rtimes Q$  with  $\mathbb{F}_l^d$  a faithful irreducible representation of  $Q$ ) or
- (b)  $G = (C_l \rtimes P_1) \times (C_l \rtimes P_2)$  with cyclic (possibly trivial)  $p$ -groups  $P_i$  that act faithfully on  $C_l \times C_l$  with  $l \neq p$  prime; or
- (4)  $G = C \rtimes P$  is quasi-elementary,  $P$  is a  $p$ -group,  $|C| = l_1 \cdots l_t$  with  $l_i \neq p$  distinct primes, the kernel  $K = \ker(P \rightarrow \text{Aut } C)$  has normal  $p$ -rank one (see Proposition 5.2). Moreover, writing  $K_j = \bigcap_{i \neq j} \ker(P \rightarrow \text{Aut } C_{l_i})$ , either
  - (a)  $K = \{1\}$  and all  $K_j$  have the same non-trivial image in the Frattini quotient of  $P$ ; or
  - (b)  $K \cong C_p$ ,  $P$  is a direct product of a group with faithful action on  $C$  by  $K$ , and the images of  $K_j$  in the Frattini quotient of  $P$  are the same for all  $j \in \{1, \dots, t\}$  and two-dimensional; or
  - (c)  $|K| > p$  or  $P$  is not a direct product by  $K$ , and the graph  $\Gamma$  attached to  $G$  by Theorem 7.29 is disconnected.

For these groups,  $\text{Prim}(G)$  is as follows. We write  $\mu$  for the Möbius function.

Case	$\text{Prim}(G)$	Basis of $\text{Prim}(G)$
1	$\mathbb{Z}/2\mathbb{Z}$	$\Theta = H - H' + ZH' - ZH$ , $H \cong C_2$ and $H' \cong C_2$ are non-conjugate non-central, $Z = Z(G) \cong C_2$
2	$(\mathbb{Z}/p\mathbb{Z})^p$	$\Theta_j = \langle y \rangle - \langle xy^j \rangle - \langle y, z \rangle + \langle xy^j, z \rangle$ , $1 \leq j \leq p$ , $G = \langle x, z \rangle \rtimes \langle y \rangle$ , $z \in Z(G)$
3a	$\mathbb{Z}$ if $Q$ cyclic $\mathbb{Z}/p\mathbb{Z}$ else ( $Q$ $p$ -quasi-elementary)	$\left. \begin{aligned} \Theta &= C_{p^k} - pQ - \mathbb{F}_l \rtimes C_{p^k} + pG \text{ if } d=1, Q=C_{p^{k+1}} \\ \Theta &= G - Q + \alpha(C_n - \mathbb{F}_l \rtimes C_n) + \beta(C_m - \mathbb{F}_l \rtimes C_m) \\ &\quad \text{if } d=1, Q=C_{mn}, \alpha m + \beta n = 1 \\ \Theta &= G - Q + \sum_U (U \rtimes N_Q U - \mathbb{F}_l^d \rtimes N_Q U) \\ &\quad \text{if } d>1; \text{ sum over } U \subset \mathbb{F}_l^d \text{ of index } l \text{ up to } G\text{-conjugacy} \\ \Theta &= \text{any relation of the form } G + \sum_{H \neq G} a_H H \end{aligned} \right\} \begin{aligned} &G \cong \mathbb{F}_l^d \rtimes Q \\ &\text{soluble} \end{aligned}$
3b	$\mathbb{Z}$ if $Q = \{1\}$ $\mathbb{Z}/p\mathbb{Z}$ if $Q \neq \{1\}$ ( $Q = P_1 \times P_2$ )	
4a	$\mathbb{Z}/p\mathbb{Z}$	$\Theta = \sum_{U \leq C} \mu( U )(MU - M'U)$ , $M, M' \leq P$ of index $p$ with signatures $(1, \dots, 1), (0, \dots, 0)$ , respectively (c.f. Prop. 7.18)
4b	$(\mathbb{Z}/p\mathbb{Z})^{p-2}$	$\Theta_i = \sum_{U \leq CK} \mu( U )(H_1 U - H_i U)$ for $1 < i < p$ , $H_j \leq P$ of index $p$ , $K \not\leq H_j$ and $(H_j \cap K_1)\Phi(P)/\Phi(P) = L_j$ , $L_j$ distinct lines in $K_1\Phi(P)/\Phi(P)$ other than $K\Phi(P)/\Phi(P)$ , $1 \leq j < p$
4c	$(\mathbb{Z}/p\mathbb{Z})^{d-1}$ $d = \#$ connected components of $\Gamma$	$\Theta_i = \sum_{U \leq CC_2^z} \mu( U )(H_1 U - H_i U)$ , $2 \leq i \leq d$ , $H_j$ any vertex in the $j$ th connected component of $\Gamma$ and $C_2^z \cong C_2 \leq Z(K)$

**1.2. Overview of the proof.** Our analysis of finite groups follows a standard pattern

abelian —  $p$ -groups — quasi-elementary — soluble — all finite,

with a somewhat surprising twist that the difficulty of understanding primitive relations seems to decrease from the middle to the sides.

It is classical that the only abelian groups that have primitive relations are  $G = C_p \times C_p$ . On the opposite side, Solomon's induction theorem together with the fact that imprimitive relations form an ideal in the Burnside ring immediately allows us to deal with a large class of groups: if  $G$  has a non-quasi-elementary quotient, then  $G$  has no primitive relations (Corollary 3.10 and Theorem 4.3(3)). Similarly, using Theorem 4.2, we get the same conclusion when  $G$  has non-cyclic quasi-elementary quotients for two distinct primes  $p \neq q$  (Theorem 4.3), and deduce Theorem A in the non-soluble case. This strategy was inspired by Deligne's work on monomial relations.

The  $p$ -group case and the soluble case are somewhat more involved. Our main tool for showing imprimitivity is the fact that in quasi-elementary groups, a relation  $\sum n_H H$  with all  $H$  contained in a proper subgroup of  $G$  is imprimitive (Proposition 3.7). This is surprisingly useful. For instance, together with Bouc's 'moving lemma' ([11] Lemma 6.15) it gives an alternative proof of the Tornehave-Bouc classification in the  $p$ -group case (see §5). The classification of primitive relations in soluble groups that are not quasi-elementary is also not hard (see §6).

The most subtle case is that of quasi-elementary groups (§7). Recall that a  $p$ -quasi-elementary group is one of the form  $G = C \rtimes P$  with  $P$  a  $p$ -group and  $C$  cyclic of order coprime to  $p$ . Assuming that such a  $G$  has a primitive relation, we analyse the kernel of the action of  $P$  on  $C$  (§7.1) and decompose all permutation representations of  $G$  explicitly into irreducible characters (§7.2). We show that  $\text{Prim}(G)$  is generated by relations of the form

$$\Theta = \sum_{U \leq C \cdot Z(G)} \mu(|U|)(UH - UH'),$$

with  $H, H' \leq G$  of maximal size among those subgroups that meet  $C \cdot Z(G)$  trivially. This already settles Theorem B below, but the remaining issue of primitivity of these generating relations is quite tricky. To show that  $\Theta$  as above is imprimitive, it is not enough to show that it is neither lifted from a quotient (e.g.  $H, H'$  do not contain a common normal subgroup of  $G$ ) nor induced from a subgroup, since  $\Theta$  could be a sum of relations each of which is either lifted or induced. It becomes necessary to explicitly split the maximal size subgroups into classes in such a way that any relation involving two subgroups from different classes has to be primitive. This is the general spirit of sections 7.3 and 7.4, which complete the proof of Theorem A.

**1.3. Remarks and applications.** Note that for non-soluble groups in Theorem A(3a),  $\text{Prim}(G)$  is generated by any relation  $\Theta = \sum_H n_H H$  with  $n_G = \pm 1$  (Theorem 4.3). An explicit construction of such a relation can be found in [30, Theorem 2.16(i)].

One of the reasons one is interested in Brauer relations comes from number theory. In fact, the motivation for the Langlands-Deligne classification of

monomial relations in soluble groups [25, 13] was to build a well-defined theory of  $\epsilon$ -factors of Galois representations starting with one-dimensional characters; to do this, one needs to prove that the  $\epsilon$ -factors of one-dimensional characters cancel in all monomial relations of local Galois groups.

If  $F/\mathbb{Q}$  is a Galois extension of number fields, arithmetic invariants of subfields  $K \subset F$  may be viewed, via the Galois correspondence  $K \leftrightarrow \text{Gal}(F/K)$ , as functions of subgroups of  $G = \text{Gal}(F/\mathbb{Q})$ . Some functions, such as the discriminant  $K \mapsto \Delta(K)$  extended to  $B(G) \rightarrow \mathbb{Q}^\times$  by linearity, factor through the representation ring  $R_{\mathbb{Q}}(G)$  and so cancel in all Brauer relations. On the other hand, the class number  $h(K)$ , the regulator  $R(K)$  or the number of roots of unity  $w(K)$  are not ‘representation-theoretic’, and do not cancel in general. However, their combination  $hR/w$  does, as it is the leading term of the Dedekind  $\zeta$ -function  $\zeta_K(s)$  at  $s = 1$ , and  $\zeta$ -functions are representation-theoretic by Artin formalism for  $L$ -functions.

Thus, Brauer relations can provide non-trivial relationships between different arithmetic invariants, like the class numbers and the regulators of various intermediate fields. This point of view proved to be very fruitful to study class numbers and unit groups [10, 24, 32, 29], related Galois module structures [9, 3] and Mordell-Weil groups and other arithmetic invariants of elliptic curves and abelian varieties [16, 15, 2]. In a slightly different direction, a verification of the vanishing in Brauer relations of *conjectural* special values of  $L$ -functions can be regarded as strong evidence for the corresponding conjectures. This has been carried out in the case of the Birch and Swinnerton-Dyer conjecture in [16] and in the case of the Bloch-Kato conjecture in [12].

One concrete number-theoretic application of Brauer relations is the theory of ‘regulator constants’, used in the proof of the Selmer parity conjecture for elliptic curves over  $\mathbb{Q}$  [16], questions related to Selmer growth [15, 17, 2], and also to analyse unit groups and higher  $K$ -groups of number fields [3, 6]. The regulator constant  $\mathcal{C}_\Theta(\Gamma) \in \mathbb{Q}^\times$  is an invariant attached to a  $\mathbb{Z}[G]$ -module  $\Gamma$  and a Brauer relation  $\Theta$  in  $G$ . For applications to elliptic curves the most important regulator constant is that of the trivial  $\mathbb{Z}[G]$ -module  $\Gamma = \mathbf{1}$ , as it controls the  $l$ -Selmer rank of the curve over the ground field. For  $\Theta = \sum n_H H$  it is simply

$$\mathcal{C}_\Theta(\mathbf{1}) = \prod_H |H|^{-n_H}.$$

To deduce something about the Selmer rank, one relies on Brauer relations in which this invariant, or rather its  $l$ -part, is non-trivial. As an application of Theorem A, in §9 we settle a question left unanswered in [16, 15, 17, 2], namely which groups have such a Brauer relation. This is done in Theorem 9.1 and Corollary 9.2; for an example of number theoretic consequences of this result, see [4].

For such applications one needs a collection of Brauer relations that span  $K(G)$  and that are ‘as simple as possible’, but whether they are imprimitive is less important. Theorem A describes the *smallest* list of groups such that

all Brauer relations in all finite groups come<sup>1</sup> from such subquotients. Let us give an alternative version of the classification theorem with a much cleaner set of generating relations, that avoids the fiddly combinatorial conditions of Theorem A (especially 4a,4b,4c). It is a direct consequence of Theorem A.

**Theorem B.** *All Brauer relations in soluble groups are generated by relations  $\Theta$  from subquotients  $G$  of the following three types. In every case,  $G$  is an extension  $1 \rightarrow C \rightarrow G \rightarrow Q \rightarrow 1$  with  $Q$  quasi-elementary and acting faithfully on  $C$ .*

- (1)  $C = \mathbb{F}_l$  (so  $G = C \rtimes Q$ ),  $H \leq G$  meets  $C$  trivially and

$$\Theta = [Q:H]G - [Q:H]Q + H - CH.$$

- (2)  $C = \mathbb{F}_l^d$  with  $d \geq 2$ ,  $G = C \rtimes Q$  and

$$\Theta = G - Q + \sum_U (U \rtimes N_Q U - \mathbb{F}_l^d \rtimes N_Q U),$$

the sum taken over representatives of  $G$ -conjugacy classes of subgroups  $U \leq \mathbb{F}_l^d$  of index  $l$ .

- (3)  $C$  is cyclic,  $Q$  is an abelian  $p$ -group,  $H, H' \leq G$  meet  $C$  trivially,  $|H| = |H'|$ , and

$$\Theta = \sum_{U \leq C} \mu(|U|)(UH - UH').$$

Conversely, all  $\Theta \in BG$  of the listed type are Brauer relations, not necessarily primitive. Finally, relations from subquotients of type (1), (3) and

- (2')  $C = S^d$  with  $d \geq 1$  and  $S$  simple,  $G$  is not quasi-elementary and

$$\Theta = \text{any relation of the form } G + \sum_{H \neq G} a_H H$$

generate all Brauer relations in all finite groups.

**Acknowledgements.** The second author is supported by a Royal Society University Research Fellowship, and the first author was partially supported by the EPSRC and is partially supported by a Research Fellowship from the Royal Commission for the Exhibition of 1851. Parts of this research were done at St Johns College, Robinson College and DPMMS in Cambridge, CRM in Barcelona, and Postech University in Pohang. We would like to thank these institutions for their hospitality and financial support. We would also like to thank Anton Evseev for making us aware of Bouc's paper. Finally, we thank an anonymous referee to pointing out to us a mistake in an earlier draft.

**1.4. Notation.** Throughout the paper,  $G$  is a finite group;  $Z(G)$  stands for the centre of  $G$  and  $\Phi(G)$  for the Frattini subgroup; whenever  $Z(G)$  is a cyclic  $p$ -group, we write  $C_p^Z$  for the central subgroup of order  $p$ ; we denote by  $\mathbf{1}$  the trivial representation; restriction from  $G$  to  $H$  and induction from  $H$  to  $G$  are denoted by  $\text{Res}_H^G \rho$  and  $\text{Ind}_H^G \sigma$ , respectively;  $H^g$  stands for  $gHg^{-1}$ .

---

<sup>1</sup>We would like to propose to use the word *indufted* instead of a vague 'come' or a cumbersome 'induced and/or lifted', but we were not brave enough to do this throughout the paper

## 2. FIRST PROPERTIES

Relations can be induced from and restricted to subgroups, and lifted from and projected to quotients as follows: let  $\Theta = \sum_i n_i H_i$  be a  $G$ -relation.

- **Induction.** If  $G'$  is a group containing  $G$ , then, by transitivity of induction,  $\Theta$  can be induced to a  $G'$ -relation  $\text{Ind}^{G'} \Theta = \sum_i n_i H_i$ .
- **Inflation.** If  $G \cong \tilde{G}/N$ , then each  $H_i$  corresponds to a subgroup  $\tilde{H}_i$  of  $\tilde{G}$  containing  $N$ , and, inflating the permutation representations from a quotient, we see that  $\tilde{\Theta} = \sum_i n_i \tilde{H}_i$  is a  $\tilde{G}$ -relation.
- **Restriction.** If  $H$  is a subgroup of  $G$ , then by Mackey decomposition  $\Theta$  can be restricted to an  $H$ -relation

$$\text{Res}_H \Theta = \sum_i \left( n_i \sum_{g \in H_i \backslash G/H} H \cap H_i^g \right).$$

On the level of  $G$ -sets this is simply the restriction of a  $G$ -set to  $H$ .

- **Projection (or deflation).** If  $N \triangleleft G$ , then  $N\Theta = \sum_i N H_i$  is a  $G/N$ -relation.

**Remark 2.1.** Note that by definition of multiplication in the Burnside ring,  $\Theta \cdot H = \text{Ind}^G(\text{Res}_H \Theta)$  for any  $G$ -relation  $\Theta$  and any subgroup  $H \leq G$ .

The number of isomorphism classes of irreducible rational representations of a finite group  $G$  is equal to the number of conjugacy classes of cyclic subgroups of  $G$  (see [28, §13.1, Cor. 1]). Since the cokernel of  $B(G) \rightarrow R_{\mathbb{Q}}(G)$  is finite (see [28, §13.1, Theorem 30]), the rank of the kernel  $K(G)$  is the number of conjugacy classes of non-cyclic subgroups.

Explicitly, Artin's induction theorem gives a relation for each non-cyclic subgroup  $H$  of  $G$ ,

$$|H| \cdot \mathbf{1} = \sum_C n_C C, \quad n_C \in \mathbb{Z},$$

the sum taken over the cyclic subgroups of  $H$ . These are clearly linearly independent, and thus give a basis of  $K(G) \otimes \mathbb{Q}$ .

**Example 2.2.** Cyclic groups have no non-zero relations.

**Example 2.3.** Let  $G = C_l \rtimes H$ , with  $l$  prime and  $H \neq \{1\}$  acting faithfully on  $C$  (so  $H$  is cyclic of order dividing  $l-1$ ). Let  $\tilde{H}$  be any subgroup of  $H$ , set  $\tilde{G} = C_l \rtimes \tilde{H}$ . Then,

$$\tilde{H} - [H : \tilde{H}] \cdot H - \tilde{G} + [H : \tilde{H}] \cdot G$$

is a relation. This can be checked by a direct computation, using the explicit description of irreducible characters of  $G$  in Remark 6.3. (See e.g. Proposition 7.12.)

**Example 2.4.** Let  $G = C_p \times C_p$ . All its proper subgroups are cyclic, so  $K(G)$  has rank one. It is generated by  $\Theta = 1 - \sum_C C + pG$ , with the sum running over all subgroups of order  $p$ , as can be checked by an explicit decomposition into irreducible characters, as above (or see Proposition 6.4).

## 3. IMPRIMITIVITY CRITERIA

**Lemma 3.1.** *Let  $G$  be a finite group, and  $\Theta = \sum_i n_i H_i$  a  $G$ -relation in which each  $H_i$  contains some non-trivial normal subgroup  $N_i$  of  $G$ . Then  $\Theta$  is imprimitive.*

*Proof.* Subtracting the projection onto  $N_1$ , we get a relation

$$\Theta - N_1 \Theta = \sum_{i, H_i \not\leq N_1} n_i (H_i - N_1 H_i),$$

which consists of subgroups each of which contains one of  $N_2, \dots, N_k$ . Repeatedly replacing  $\Theta$  by  $\Theta - N_j \Theta$  we see that the remaining relation is zero, so  $\Theta$  is a sum of relations that are lifted from quotients.  $\square$

**Lemma 3.2.** *Let  $G \not\cong C_p \times C_p$  be a finite group with non-cyclic centre. Then  $G$  has no primitive relations.*

*Proof.* Let  $Z = C_p \times C_p \leq Z(P)$ . For any  $H \leq G$  that intersects  $Z$  trivially,  $HZ/H \cong C_p \times C_p$ . By lifting the relation of Example 2.4 to  $HZ$  and then inducing to  $G$ , we can replace any occurrence of  $H$  in any  $G$ -relation by groups that intersect  $Z$  non-trivially, using imprimitive relations. Each such intersection is normal in  $G$ , so by Lemma 3.1 the resulting relation is imprimitive as well.  $\square$

We will now develop criteria for a relation to be induced from a subgroup.

**Proposition 3.3.** *Let  $G$  be a finite group and  $D \leq G$  a subgroup for which the natural map  $B(D) \rightarrow B(G)$  is injective. If  $\Theta = \sum_i n_i H_i$  is a  $G$ -relation with  $H_i \leq D$  for all  $i$ , then  $\Theta$  is induced from a  $D$ -relation.*

*Proof.* First, we claim that the image of  $\text{Ind} : K(D) \rightarrow K(G)$  is a saturated sublattice, i.e. that if  $\Theta$  is induced from a  $D$ -relation and  $R$  is a  $G$ -relation such that  $\Theta = nR$  for some integer  $n$ , then  $R$  is induced from a  $D$ -relation (and not just from an element of the Burnside ring of  $D$ , which is trivially true). Indeed, it is enough to show that the image of the induction map  $\text{Ind} : K(D) \rightarrow B(G)$  is saturated. But it is a composition of the two injections  $K(D) \rightarrow B(D) \xrightarrow{\text{Ind}} B(G)$  whose images are clearly saturated, and so it has saturated image.

The image  $\mathcal{Y}$  of  $\text{Ind} : K(D) \rightarrow K(G)$  is obviously contained in the space  $\mathcal{X}$  of  $G$ -relations  $\sum_i n_i H_i$  for which  $H_i \leq D$  for all  $i$ . So we only need to compare the ranks of the two spaces.

We have already remarked that the rank of  $K(G)$  is equal to the number of conjugacy classes of non-cyclic subgroups of  $G$ , a basis for  $K(G) \otimes \mathbb{Q}$  obtained by applying Artin's induction theorem to a representative of each conjugacy class of non-cyclic subgroups of  $G$ . Hence, it is immediate that a basis for  $\mathcal{X} \otimes \mathbb{Q}$  is given by the subset of this set corresponding to those conjugacy classes of non-cyclic subgroups that have a representative lying in  $D$ . But all these relations are clearly contained in  $\mathcal{Y} \otimes \mathbb{Q}$ , so  $\mathcal{X} \otimes \mathbb{Q} \subseteq \mathcal{Y} \otimes \mathbb{Q}$  and we are done.  $\square$

**Proposition 3.4.** *Let  $G$  be a finite group, and  $N \triangleleft G$  a normal subgroup of prime index that is either metabelian or supersolvable. If  $\Theta = \sum_i n_i H_i$  is a  $G$ -relation with all  $H_i \leq N$ , then  $\Theta$  is induced from an  $N$ -relation.*



**Remark 3.5.** It is not true that  $\sum_i n_i H_i$  is a  $D$ -relation, since the  $H_i$  are representatives of  $G$ -conjugacy classes of subgroups and they might represent the “wrong”  $D$ -conjugacy classes. For example, if  $H_1$  and  $H_1^g$  are not conjugate in  $D$ , then  $H_1 - H_1^g$  will not be a  $D$ -relation in general, while it is the zero element in the Burnside ring of  $G$  and in particular a  $G$ -relation.

*Proof.* Write  $p$  for the index of  $N$  in  $G$ , and fix a generator  $T$  of the quotient  $G/N \cong C_p$ . Recall (see e.g. [1] §8) that for a  $C_p$ -module  $M$ ,

$$H^1(C_p, M) = \frac{\text{1-cocycles}}{\text{1-coboundaries}} = \frac{\ker(1 + T + \dots + T^{p-1})}{\text{Im}(1 - T)}.$$

Let  $\Theta = \sum_i n_i H_i$  be a  $G$ -relation with  $H_i \leq N$  for all  $i$ ; we view it as an element of the Burnside ring of  $N$ . Write  $\tilde{\Theta} = \sum m_\rho \rho$  for its image in the rational representation ring  $R_{\mathbb{Q}}(N)$ , the sum taken over the irreducible<sup>2</sup> representations of  $N$ . Note that  $\text{Ind}_N^G \tilde{\Theta} = 0$ , since  $\Theta$  is a  $G$ -relation.

We need to show that we can add to  $\Theta$  a linear combination of terms of the form  $H^g - H$  for  $H \leq N, g \in G$  such that the resulting element of  $B(N)$  is an  $N$ -relation. In other words, we claim that  $\Theta$  is a coboundary for the action of  $G/N$  on  $M = B(N)/K(N)$ ; note that  $G$  acts naturally on  $B(N)$  and  $K(N)$ , with  $N$  acting trivially.

Given any two irreducible representations  $\rho_1, \rho_2$  of  $N$ , Clifford theory says that  $\text{Ind}_N^G \rho_1 \cong \text{Ind}_N^G \rho_2$  if  $\rho_1, \rho_2$  are in the same  $G$ -orbit, and disjoint otherwise. This is classical over  $\mathbb{C}$ , and over  $\mathbb{Q}$  it follows from the fact that complex irreducible representations  $\chi_1, \chi_2$  of  $N$  are in the same  $G$ -orbit if and only if their rational hulls are in the same  $G$ -orbit. Therefore, for every irreducible representation  $\tau$  of  $G$ ,

$$0 = \langle \tau, \text{Ind}_N^G \tilde{\Theta} \rangle = \sum_{\rho} m_{\rho} \langle \tau, \text{Ind}_N^G \rho \rangle = c \sum_{\substack{\rho: \\ \langle \tau, \text{Ind}_N^G \rho \rangle \neq 0}} m_{\rho},$$

where  $c = \langle \tau, \text{Ind}_N^G \rho \rangle$  for any  $\rho$  for which this inner product is non-zero.

We will now show that the condition that  $\sum_{\rho: \langle \tau, \text{Ind}_N^G \rho \rangle \neq 0} m_{\rho} = 0$  for every  $\tau$  is a cocycle condition for the action of  $G/N$  on  $M$ , and that every cocycle is a coboundary.

As remarked above, the irreducible representations  $\rho$  of  $N$  for which  $\langle \tau, \text{Ind}_N^G \rho \rangle \neq 0$  form one complete  $G$ -orbit  $\{\rho, \rho^T, \dots, \rho^{T^{p-1}}\}$  (of size 1 or  $p$ ). In other words,  $\tilde{\Theta} \in R_{\mathbb{Q}}(N)$  is annihilated by the operator  $1 + T + T^2 + \dots + T^{p-1}$ , so it is indeed a 1-cocycle for the action of  $C_p$  on  $M$ , viewing  $M$  as a submodule of  $R_{\mathbb{Q}}(N)$ . It remains to prove that

$$H^1(G/N, M) = 0.$$

Any irreducible representation of  $N$  is either fixed by  $G$  or has orbit of size  $p$ . Thus,  $R_{\mathbb{Q}}(N)$  as a  $G/N$ -module is a direct sum of trivial modules  $\mathbb{Z}$  and of regular modules  $\mathbb{Z}[C_p]$ . The module  $M$ , viewed as the image of  $B(N)$  in  $R_{\mathbb{Q}}(N)$ , is of finite index in  $R_{\mathbb{Q}}(N)$  by Artin’s induction theorem. Since  $N$  is either metabelian or supersolvable, a theorem of Berz [8, 22] says that  $M$  is spanned by elements of the form  $a_{\phi} \phi$ , as  $\phi$  runs over the irreducible

<sup>2</sup>Throughout the proof the word ‘irreducible’ refers to a rational representation, irreducible over  $\mathbb{Q}$ .

representations of  $N$ , for suitable  $a_\phi \in \mathbb{N}$ . Note that  $a_\phi = a_{\phi^T}$ , because  $M \leq R_{\mathbb{Q}}(N)$  is a  $C_p$ -submodule. It follows that  $M$  is also a direct sum of trivial and of regular  $C_p$ -modules. Now  $H^1(C_p, \mathbb{Z}) = \text{Hom}(C_p, \mathbb{Z}) = 0$ , and also  $H^1(C_p, \mathbb{Z}[C_p]) = 0$  since  $\mathbb{Z}[C_p] \cong \text{Hom}_{C_p}(\mathbb{Z}[C_p], \mathbb{Z})$  is co-induced. As  $H^1$  is additive in direct sums, we get that  $H^1(C_p, M) = 0$ , as claimed.  $\square$

**Definition 3.6.** A group is called *p-quasi-elementary* if it has a normal cyclic subgroup whose quotient is a  $p$ -group. It is called *quasi-elementary* if it is  $p$ -quasi-elementary for some prime  $p$ .

**Proposition 3.7.** *Let  $G$  be a quasi-elementary group, let  $D$  be a proper subgroup. Let  $\Theta = \sum_i n_i H_i$  be a  $G$ -relation such that  $H_i \leq D$  for all  $i$ . Then  $\Theta$  is induced from some proper subgroup of  $G$ , and in particular is imprimitive.*

*Proof.* Write  $G = C \rtimes P$ , with  $P$  a  $p$ -group and  $C$  cyclic of order prime to  $p$ .

It suffices to prove the proposition for maximal subgroups  $D$  of  $G$ . Every maximal subgroup of  $G$  is either conjugate to  $D = C \rtimes S$  with  $S \triangleleft P$  of index  $p$ , or to  $D = U \rtimes P$  where  $U$  is a maximal subgroup of  $C$ . In the former case,  $D \triangleleft G$  is of prime index and is quasi-elementary and therefore supersolvable, so the corollary follows from Proposition 3.4. Assume that we are in the latter case, let  $D$  have prime index  $l$  in  $G$ . We will show that the map  $B(D) \rightarrow B(G)$  is injective, and the claim will follow from Proposition 3.3.

In general, the kernel of the induction map  $B(D) \rightarrow B(G)$  is generated by elements of the form  $H - H^g$  where  $H, H^g \leq D$  are not  $D$ -conjugate. We therefore have to verify that two  $G$ -conjugate subgroups  $H, H^g \leq D = U \rtimes P$  are necessarily  $D$ -conjugate.

Because  $G = C_{l^k} D$  for some  $k \geq 1$ , we can write  $g = cd, c \in C_{l^k}, d \in D$ , so  $H^g = (H^d)^c$ . Replacing  $H$  by  $H^d$  (which is still a subgroup of  $D$ ), we may assume that  $g = c \in C_{l^k}$ . If the order of  $c$  is less than  $l^k$ , then  $c \in D$ , and we are done. So assume that  $c$  has order  $l^k$ . If  $H$  commutes with  $C_{l^k}$ , then  $H = H^c$ , and the claim is trivial. Otherwise, there exists  $h \in H$  (without loss of generality of order coprime to  $l$ ) for which  $hch^{-1} = c^i$  for some  $i \not\equiv 1 \pmod{l}$ . But then  $h^c h^{-1} = chc^{-1} h^{-1} = c^{1-i}$  still has order  $l^k$ , and therefore cannot lie in  $D$ , contradicting the assumption that  $H, H^c \leq D$ .  $\square$

**Corollary 3.8.** *Let  $G$  be a quasi-elementary group and let  $\{1\} \neq N_j \triangleleft G$ ,  $N_j \leq D \leq G$ ,  $j = 1, \dots, s$ . If  $\Theta = \sum_i n_i H_i$  is a  $G$ -relation with the property that for each  $H_i$  either  $H_i \geq N_j$  for some  $j$  or  $H_i \leq D$ , then  $\Theta$  is imprimitive.*

*Proof.* Let  $\Theta_0 = \Theta$  and define inductively  $\Theta_j = \Theta_{j-1} - N_j \Theta_{j-1}$  for  $1 \leq j \leq s$ . Then  $\Theta_s$  consists only of subgroups of  $D$ , so it is imprimitive by Proposition 3.7. Because the projections  $N_j \Theta_{j-1}$  are lifted from  $G/N_j$ , they are also imprimitive.  $\square$

**Lemma 3.9.** *Let  $G$  be a finite group and  $R$  any Brauer relation in  $G$ , possibly 0. Then the  $\mathbb{Z}$ -span of all imprimitive relations and  $R$  is an ideal in the Burnside ring of  $G$ .*

*Proof.* If  $H \neq G$ , then  $H \cdot \Theta = \text{Ind}_H^G \text{Res}_H \Theta$  is imprimitive for any relation  $\Theta$ . If, on the other hand,  $H = G$ , then  $H \cdot \Theta = \Theta$ .  $\square$

**Corollary 3.10.** *Let  $G$  be a finite group and suppose that there exists an imprimitive  $G$ -relation  $R$  in which  $G$  enters with coefficient 1. Then  $G$  has no primitive relations.*

*Proof.* If  $\Theta = \sum_i n_i H_i$  is any relation, then  $R \cdot \Theta = \Theta - \sum_H n_H \text{Ind}^G \text{Res}_H \Theta$ . By Lemma 3.9,  $R \cdot \Theta$  is imprimitive, and clearly  $\sum_H n_H \text{Ind}^G \text{Res}_H \Theta$  is also a sum of imprimitive relations.  $\square$

#### 4. A CHARACTERISATION IN TERMS OF QUOTIENTS

The main result of this section, Theorem 4.3, gives a characterisation of  $\text{Prim}(G)$  in terms of the existence of quasi-elementary quotients of  $G$ . First recall Solomon's induction theorem and a statement complementary to it:

**Theorem 4.1** (Solomon's induction theorem). *Let  $G$  be a finite group. There exists a Brauer relation of the form  $G - \sum_H n_H H$  where the sum runs over quasi-elementary subgroups of  $G$  and  $n_H$  are integers.*

**Theorem 4.2** ([14]). *Let  $G$  be a non-cyclic  $p$ -quasi-elementary group. Then there exists a relation in which  $G$  enters with coefficient  $p$ . Moreover, in any  $G$ -relation the coefficient of  $G$  is divisible by  $p$ .*

**Theorem 4.3.** *Let  $G$  be a non-quasi-elementary group.*

- (1)  $\text{Prim}(G) \cong \mathbb{Z}$  if all proper quotients of  $G$  are cyclic.
- (2)  $\text{Prim}(G) \cong \mathbb{Z}/p\mathbb{Z}$  if all proper quotients of  $G$  are  $p$ -quasi-elementary for the same prime  $p$ , and at least one of them is not cyclic.
- (3)  $\text{Prim}(G) = 0$  otherwise.

*In cases (1) and (2),  $\text{Prim}(G)$  is generated by any relation in which  $G$  has coefficient 1.*

*Proof.* By Solomon's induction theorem,  $G$  has a relation of the form  $R = G - \sum_{H \neq G} n_H H$ , and we claim that  $R$  generates  $\text{Prim}(G)$  in all cases. By Lemma 3.9, the span  $I$  of the set of imprimitive relations and of  $R$  is an ideal in  $B(G)$ . To show that  $K(G) \subset I$ , let  $\Theta$  be any relation. Then  $\Theta = R \cdot \Theta + (\Theta - R \cdot \Theta)$  and  $R \cdot \Theta \in I$ . Also,

$$\Theta - R \cdot \Theta = \sum_{H \neq G} n_H (\Theta \cdot H)$$

is imprimitive and therefore also in  $I$ . So  $\Theta \in I$ , as claimed.

It remains to determine the smallest integer  $n > 0$  such that  $G$  has an imprimitive relation of the form  $\Theta = nG - \sum_{H \neq G} m_H H$ . Then  $\text{Prim}(G) \cong \mathbb{Z}/n\mathbb{Z}$  (and  $\mathbb{Z}$  if there is no such  $n$ ). Clearly  $G$  does not enter the relations that are induced from proper subgroups, so such a  $\Theta$  must be a linear combination of relations lifted from proper quotients.

- (1) If all proper quotients of  $G$  are cyclic, there are no such relations.
- (2) If all proper quotients are  $p$ -quasi-elementary, then  $n$  is a multiple of  $p$  by Theorem 4.2, and there is a relation with  $n = p$  by the same theorem if one of them is not cyclic.
- (3) Otherwise, either
  - (a) some proper quotient  $G/N$  is not quasi-elementary, in which case we apply Solomon's induction to  $G/N$  and lift the resulting relation to  $G$ ; or

- (b)  $G$  has two proper non-cyclic quotients  $G/N_1, G/N_2$  which are  $p$ - and  $q$ -quasi-elementary with  $p \neq q$ , in which case we take a linear combination of the two lifted relations  $pG + \dots$  and  $qG + \dots$ .

In both cases, there is an imprimitive relation with  $n=1$ , so  $\text{Prim}(G)=0$ .  $\square$

**Corollary 4.4.** *If a finite group  $G$  has a primitive relation, then there is a prime  $p$  such that every proper quotient of  $G$  is  $p$ -quasi-elementary.*

*Proof.* If  $G$  itself is  $p$ -quasi-elementary, then so are all its quotients, and there is nothing to prove. Otherwise, apply the theorem.  $\square$

**Corollary 4.5.** *Let  $G$  be a finite group that has a primitive relation. Then  $G$  is an extension of the form*

$$(4.6) \quad 1 \rightarrow S^d \rightarrow G \rightarrow Q \rightarrow 1, \quad d \geq 1$$

*with  $S$  a simple group and  $Q$   $p$ -quasi-elementary. Moreover, if  $S$  is not cyclic (equivalently if  $G$  is not soluble), then the canonical map  $Q \rightarrow \text{Out}(S^d)$  is injective and  $S^d$  has no proper non-trivial subgroups that are normal in  $G$ . In this case,  $\text{Prim}(G) \cong \mathbb{Z}$  if  $Q$  is cyclic and  $\text{Prim}(G) \cong \mathbb{Z}/p\mathbb{Z}$  otherwise.*

*Proof.* By the existence of chief series for finite groups, any  $G \neq \{1\}$  is an extension (4.6) of some  $Q$ , with simple  $S$ . Because  $G$  has a primitive relation,  $Q$  is quasi-elementary by Theorem 4.3.

Now suppose  $S$  is not cyclic, and consider the kernel  $K$  of the map  $G \rightarrow \text{Aut}(S^d)$  given by conjugation. The centre of  $S^d$  is trivial, so  $K \cap S^d = \{1\}$ . If  $K \neq \{1\}$ , then  $G/K$  is a proper non-quasi-elementary quotient, contradicting Theorem 4.3. So  $G \hookrightarrow \text{Aut}(S^d)$  and, factoring out  $S^d \cong \text{Inn}(S^d)$ , we get  $Q \hookrightarrow \text{Out}(S^d)$ . In the same way, if  $N \triangleleft G$  is a proper subgroup of  $S^d$ , then  $G/N$  is not quasi-elementary, so again  $N = \{1\}$ .

Finally, the description of  $\text{Prim}(G)$  is given by Theorem 4.3.  $\square$

**Remark 4.7.** Conversely, suppose that  $G$  is an extension as in (4.6) with  $p$ -quasi-elementary  $Q$ , non-cyclic  $S$  and  $Q \hookrightarrow \text{Out}(S^d)$ . Suppose also that  $S^d$  has no proper non-trivial subgroups that are normal in  $G$ . It follows that every non-trivial normal subgroup of  $G$  contains  $S^d$ . So  $G$  is not quasi-elementary but every proper quotient of it is, and therefore  $G$  has a primitive relation. This proves Theorem A for all non-soluble groups.

## 5. PRIMITIVE RELATIONS IN $p$ -GROUPS

**Definition 5.1.** The normal  $p$ -rank of a finite group  $G$  is the maximum of the ranks of the elementary abelian normal  $p$ -subgroups of  $G$ .

As in Bouc's work [11], the groups of normal  $p$ -rank one will be of particular importance to us. We will repeatedly need the following classification:

**Proposition 5.2** ([20], Theorem 5.4.10). *Let  $P$  be a  $p$ -group with normal  $p$ -rank one. Then  $P$  is one of the following:*

- the cyclic group  $C_{p^n} = \langle c | c^{p^n} = 1 \rangle$ ;
- the dihedral group  $D_{2n+1} = \langle c, x | c^{2^n} = x^2 = 1, xcx = c^{-1} \rangle$  with  $n \geq 3$ ;
- the generalised quaternions,  $Q_{2n+2} = \langle c, x | c^{2^n} = x^2, x^{-1}cx = c^{-1} \rangle$  with  $n \geq 1$ ;

- the semi-dihedral group  $SD_{2^{n+1}} = \langle c, x | c^{2^n} = x^2 = 1, xcx = c^{2^{n-1}-1} \rangle$  with  $n \geq 3$ .

We now present an alternative proof of the Tornehave–Bouc theorem ([11], Cor. 6.16). The ingredients are the results of §3 and a lemma of Bouc [11, Lemma 6.15].

**Theorem 5.3** (Tornehave–Bouc). *All Brauer relations in  $p$ -groups are  $\mathbb{Z}$ -linear combinations of ones lifted from subquotients  $P$  of the following types:*

- (i)  $P \cong C_p \times C_p$  with the relation  $1 - \sum_C C + p \cdot P$ , the sum taken over all subgroups of order  $p$ ;
- (ii)  $P$  is the Heisenberg group of order  $p^3$ , and the relation is  $I - IZ - J + JZ$  where  $Z = Z(P)$  and  $I$  and  $J$  are two non-conjugate non-central subgroups of order  $p$ ;
- (iii)  $P \cong D_{2^n}$  with the relation  $I - IZ - J + JZ$ , where  $Z = Z(P)$  and  $I$  and  $J$  are two non-conjugate non-central subgroups of order 2.

*Proof.* Let  $P$  be a  $p$ -group that has a primitive relation. By Lemma 3.2, either  $P = C_p \times C_p$  or  $P$  has cyclic centre. The former case is covered by Example 2.4, so assume that we are in the second case, and let  $C_p^z$  be the unique central subgroup of order  $p$ .

First, suppose  $P$  has normal  $p$ -rank  $r \geq 2$ , with  $V = (C_p)^r \triangleleft P$ . The conjugation action of  $P$  on  $V$  is upper-triangular, as is any action of a  $p$ -group on an  $\mathbb{F}_p$ -vector space. So there are normal subgroups  $(C_p)^j \triangleleft G$  for all  $j \leq r$ , and we denote by  $E$  one for  $j = 2$ . Note that  $C_p^z \subset E$ , since any normal subgroup of a  $p$ -group meets its centre. By [11, Lemma 6.15], any occurrence in a relation of a subgroup that does not contain  $C_p^z$  and is not contained in the centraliser  $C_P(E)$  of  $E$  in  $P$  can be replaced by subgroups that either contain  $C_p^z$  or are contained in  $C_P(E)$ , using a relation from a subquotient isomorphic to the Heisenberg group of order  $p^3$ . The remaining relation is then imprimitive by Corollary 3.8. So  $P$  has a primitive relation if and only if it is the Heisenberg group of order  $p^3$ .

Now suppose that  $r = 1$ , so  $P$  is as in 5.2. If  $P$  is cyclic or generalised quaternion, then every non-trivial subgroup contains  $C_p^z$ , so  $P$  has no primitive relations by Corollary 3.8. If  $P$  is semi-dihedral, then the only conjugacy class of non-trivial subgroups of  $P$  that do not contain  $C_2^z$  is that of non-central involutions, represented by  $\langle x \rangle$ , say. But  $x$  and  $C_2^z$  generate a proper subgroup of  $P$ , so  $P$  again has no primitive relations by Corollary 3.8. Finally, if  $P$  is dihedral, then there are two conjugacy classes of non-trivial subgroups that do not contain  $C_2^z$ , represented, say, by  $I$  and  $J$ . Using the relation in (iii) (cf. [11, page 25]) any occurrence of  $I$  in a relation can be replaced by  $J$  and by subgroups that contain  $C_2^z$ . In the resulting relation, every subgroup will either contain  $C_2^z$  or will be contained in  $D = C_2^z \times J$ , which is a proper subgroup of  $P$ . So, applying Corollary 3.8 again, we see that the group of primitive relations of  $P$  is generated by the relation of (iii) and the theorem is proved.  $\square$

## 6. MAIN REDUCTION IN SOLUBLE GROUPS

**Theorem 6.1.** *Every finite soluble group that has a primitive relation is either*

- (i) *quasi-elementary, or*
- (ii) *of the form  $(C_l)^d \rtimes Q$  where  $Q$  is quasi-elementary and acts faithfully and irreducibly on the  $\mathbb{F}_l$ -vector space  $(C_l)^d$  by conjugation, or*
- (iii) *of the form  $(C_l \rtimes P_1) \times (C_l \rtimes P_2)$  with cyclic  $p$ -groups  $P_i \hookrightarrow \text{Aut } C_l$ .*

*Proof.* Since  $G$  is soluble and has a primitive relation, by Corollary 4.5 it is an extension of the form

$$(6.2) \quad 1 \rightarrow (C_l)^d \rightarrow G \rightarrow Q \rightarrow 1, \quad d \geq 1,$$

with  $Q$  quasi-elementary. If  $Q = \{1\}$ , then we are in case (i). So, assume that  $Q \neq \{1\}$ , and consider the various possibilities for the structure of  $Q$  and its action on  $W = (C_l)^d$  by conjugation.

**(A)** *Suppose that  $l$  does not divide  $|Q|$ .* The sequence (6.2) then splits by the Schur–Zassenhaus theorem, so  $G = W \rtimes Q$ . The kernel of the action of  $Q$  on  $W$  is then a normal subgroup  $N \triangleleft G$ .

**Case 1:  $N \neq \{1\}$  and  $Q$  is cyclic.** By Corollary 4.4,  $G/N$  is quasi-elementary. If it is  $p$ -quasi-elementary for some  $p \neq l$ , then its  $l$ -part must be cyclic, so  $d = 1$ . Moreover, since  $Q/N$  acts faithfully on  $C_l$ , it must be a  $p$ -group. So, writing  $Q = Q_p \times Q_{p'}$ , where  $Q_p$  is the Sylow  $p$ -subgroup of  $Q$ , we deduce that  $N$  contains  $Q_{p'}$ , which is cyclic of order coprime to  $l$ , and so  $G = (C_l \times Q_{p'}) \rtimes Q_p$  is quasi-elementary (case (i)). If  $G/N$  is  $l$ -quasi-elementary, then  $l \nmid |Q|$  implies that  $Q/N \triangleleft G/N$ , so  $G/N = (Q/N) \times W$ . But  $N$  is the whole kernel of the action of  $Q$  on  $W$ , so  $Q/N$  must be trivial. In this case  $Q = N$  is normal in  $G$ , and  $G = Q \times W$  is again quasi-elementary.

**Case 2:  $N \neq \{1\}$  and  $Q$  is not cyclic.** Write  $Q = C \rtimes P$  with  $C$  cyclic of order coprime to  $lp$  and  $P$  a  $p$ -group. This time, we know that  $G/N$  is  $p$ -quasi-elementary by Corollary 4.4. Since  $p \neq l$ , we have  $d = 1$ . Also, because  $G/N$  is  $p$ -quasi-elementary and the action of  $Q/N$  on  $C_l$  is faithful,  $Q/N$  must be a  $p$ -group. So  $N$  contains  $C$ , and  $G = (C_l \times C) \rtimes P$  is  $p$ -quasi-elementary.

**Case 3:  $N = \{1\}$  and  $Q$  acts reducibly.** Since  $l \nmid |Q|$ , the  $\mathbb{F}_l$ -representation  $W$  of  $Q$  is completely reducible. Say  $W = \bigoplus_{i=1}^n V_i$  with irreducible  $V_i$ ; so  $V_i \triangleleft G$ .

Let  $p$  be a prime divisor of  $|Q|$ . A Sylow  $p$ -subgroup of  $Q$  acts faithfully on  $W$ , so it acts non-trivially on one of the  $V_i$ , say on  $V_1$ . Because  $U = G/(V_2 \oplus \cdots \oplus V_n) \cong V_1 \rtimes Q$  is quasi-elementary by Corollary 4.4, and because its  $p$ -Sylow is not normal in it,  $U$  must be  $p$ -quasi-elementary (and not cyclic). However, Corollary 4.4 asserts that all proper non-cyclic quotients of  $G$  are quasi-elementary with respect to the same prime, so  $|Q|$  cannot have more than one prime divisor. In other words,  $Q$  is a  $p$ -group.

Now, both  $G/V_1$  and  $G/V_2$  must be  $p$ -quasi-elementary, so their  $l$ -parts are cyclic. This is only possible if  $n = 2$  and  $\dim V_1 = \dim V_2 = 1$ . So  $W = C_l \times C_l$ , and

$$P \hookrightarrow (\text{Aut } C_l) \times (\text{Aut } C_l) \cong \mathbb{F}_l^\times \times \mathbb{F}_l^\times$$

is an abelian  $p$ -group. This is case (iii) of the theorem.

**Case 4:  $N = \{1\}$  and  $Q$  acts irreducibly.** This is case (ii).

**(B)** *Suppose that  $l$  divides  $|Q|$ .* Again, consider several cases:

**Case 5:  $Q$  is cyclic.** Write  $Q = Q_l \times Q_{l'}$  with  $Q_l$  the Sylow  $l$ -subgroup of  $Q$ , so  $G = L \rtimes Q_{l'}$  for an  $l$ -group  $L$ . If the derived subgroup  $L'$  is non-trivial, then  $G/L' \cong L/L' \rtimes Q_{l'}$  must be quasi-elementary. If it is  $p$ -quasi-elementary for  $p \neq l$ , then  $L/L'$  must be cyclic, so  $L$  is cyclic, contradicting the assumption that  $L' \neq \{1\}$ . If it is  $l$ -quasi-elementary, then  $Q_{l'}$  acts trivially on  $L/L'$ . By a classical theorem of Burnside, the kernel of  $\text{Aut}(L) \rightarrow \text{Aut}(L/L')$  is an  $l$ -group. Since  $Q_{l'}$  is of order coprime to  $l$ , we deduce that it acts trivially on  $L$ , so  $G = L \times Q_{l'}$ , and is thus quasi-elementary. Finally, suppose that  $L$  is abelian. It is either an  $\mathbb{F}_l$ -vector space or the Frattini subgroup  $\Phi(L)$  of  $L$  is a non-trivial normal subgroup of  $G$ . In the latter case, by exactly the same argument, either  $L/\Phi(L) \rtimes Q_{l'}$  is  $p$ -quasi-elementary, in which case so is  $G$ , or  $G$  is  $l$ -quasi-elementary. In summary,  $G$  is either quasi-elementary or  $L$  is an  $\mathbb{F}_l$ -vector space and we are in (A).

**Case 6:  $Q$  is non-cyclic  $p$ -quasi-elementary for  $p \neq l$ .** So  $Q = C \rtimes P$  with  $P$  a  $p$ -group and  $C$  cyclic of order divisible by  $l$ . Write  $C = U_l \times U_{l'}$  where  $U_l$  is the Sylow  $l$ -subgroup of  $C$ . Then  $G = L \rtimes (U_{l'} \rtimes P)$ , where  $L = WU_l$  is an  $l$ -group. Again, consider the derived subgroup  $L'$  of  $L$ . If  $L' \neq \{1\}$ , then  $G/L' \cong L/L' \rtimes (U_{l'} \rtimes P)$  is  $p$ -quasi-elementary by Corollary 4.4, so  $L/L'$  is cyclic and thus so is  $L$ , giving a contradiction. Therefore,  $L$  must be abelian. If  $\Phi(L)$  is not trivial, then  $G/\Phi(L)$  is  $p$ -quasi-elementary, so  $L \rtimes U_{l'}$  is cyclic and  $G$  is quasi-elementary. Otherwise,  $L$  is an  $\mathbb{F}_l$ -vector space and we are in (A).

**Case 7:  $Q$  is non-cyclic  $l$ -quasi-elementary.** Now  $Q = C \rtimes P$  with  $C$  cyclic of order prime to  $l$ , and  $P$  an  $l$ -group, both non-trivial.

First, consider the case  $d = 1$ . We claim, that in this case, either  $C$  acts faithfully on  $W$  or  $G$  is  $l$ -quasi-elementary. Indeed, let  $K$  be the kernel of the action of  $C$  on  $W$ , and suppose that  $K \neq \{1\}$ . Then  $K$  is normal in  $G$  and  $G/K$  must be  $l$ -quasi-elementary, so  $C/K$  acts trivially on  $W$ . But  $K$  was assumed to be the whole kernel so  $K = C$  and  $G = (C_l \times C) \rtimes P$  is  $l$ -quasi-elementary. But also, if  $C$  acts faithfully, then it is a subgroup of  $\mathbb{F}_l^\times$  and the  $l$ -group  $P$  cannot act on  $C$  non-trivially, so  $G = (C_l \times C) \times P$ . By Corollary 4.4,  $C_l \rtimes C \cong G/P$  must be  $l$ -quasi-elementary, contradicting the faithfulness of the action of  $C$ .

So, now suppose that  $d > 1$ . We first claim that if  $W$  is irreducible as a  $Q$ -representation, then the extension of  $Q$  by  $W$  splits. First, observe that the invariant subspace  $W^C$  is zero. For if not, then it is an  $\mathbb{F}_l$ -vector space with an action of the  $l$ -group  $P$ , which must have a fixed vector. This vector would span a  $Q$ -invariant subspace, contradicting irreducibility. Now consider the inflation-restriction sequence for  $C \triangleleft Q$  acting on  $W$ :

$$H^2(Q/C, W^C) \longrightarrow H^2(Q, W) \longrightarrow H^2(C, W).$$

The first group is zero as  $W^C = 0$ , and the last one is zero as it is killed by  $|C|$  and by  $|W|$ , which are coprime. So the middle group, which classifies extensions of  $Q$  by  $W$  up to splitting, is zero and the claim is established.

We can now proceed as in (A): if  $N \neq \{1\}$  is the kernel of the action of  $Q$  on  $W$ , then it is a normal subgroup of  $G$  and  $G/N$  is  $l$ -quasi-elementary, which implies that  $C$  is normal in  $G$  and so  $G$  is  $l$ -quasi-elementary. If, on the other hand, the kernel is trivial, then we are in case (ii).

Finally, suppose that the representation  $W$  is reducible, and let  $0 \subsetneq V \subsetneq W$  be a subrepresentation. Since  $G/V$  is  $l$ -quasi-elementary,  $C$  must act trivially on  $W/V$ . But  $W$  is an ordinary representation of  $C$ , so there exists a subspace of  $W$  invariant under  $C$ . Since  $W^C$  is also a  $P$ -representation, it is a non-trivial subrepresentation of  $W$ . But by the same argument,  $C$  must also act trivially on  $W/W^C$ , so using complete reducibility again, we deduce that  $C$  acts trivially on  $W$  and  $G$  is  $l$ -quasi-elementary.  $\square$

**Remark 6.3.** Before continuing, we will recall from [28, §8.2] the classification of irreducible characters of semi-direct products by abelian groups. Let  $G = A \rtimes H$  with  $A$  abelian. The group  $H$  acts on 1-dimensional characters of  $A$  via

$$h(\chi)(a) = \chi(hah^{-1}), \quad h \in H, a \in A, \chi : A \rightarrow \mathbb{C}^\times.$$

Let  $X$  be a set of representatives of  $H$ -orbits of these characters. For  $\chi \in X$  write  $H_\chi$  for its stabiliser in  $H$ . Then  $\chi$  can be extended to a one-dimensional character of its stabiliser  $S_\chi = A \rtimes H_\chi$  in  $G$ . Let  $\rho$  be an irreducible character of  $H_\chi \cong S_\chi/A$  and lift it to  $S_\chi$ . Then  $\text{Ind}^G(\chi \otimes \rho)$  is an irreducible character of  $G$  and all irreducible characters of  $G$  arise uniquely in this way, for varying  $\chi \in X$  and  $\rho$ .

**Proposition 6.4.** *Let  $G = W \rtimes H$  with  $W \cong (C_l)^d$  for  $d \geq 2$ , and  $H$  acting faithfully on  $W$ . Let  $\mathcal{U}$  be a set of representatives of the  $G$ -conjugacy classes of hyperplanes  $U \subset W$ , and write  $H_U = N_H(U)$  for  $U \in \mathcal{U}$ . Then*

$$\Theta = G - H + \sum_{U \in \mathcal{U}} (H_U U - H_U W)$$

is a  $G$ -relation.

*Proof.* We retain the notation of Remark 6.3 for the irreducible characters of  $G$ . Choose the set  $X$  of representatives for the  $H$ -orbits of 1-dimensional characters of  $W$  in such a way that  $\ker \chi \in \mathcal{U}$  for  $\mathbf{1} \neq \chi \in X$ .

To prove that  $\Theta$  is a relation, it suffices to show that

$$\begin{aligned} \mathbb{C}[G/H] \ominus \mathbf{1} &= \bigoplus_{\chi \in X, \chi \neq \mathbf{1}} \text{Ind}^G(\chi \otimes \mathbf{1}_{H_\chi}), \\ \mathbb{C}[G/H_U U] \ominus \mathbb{C}[G/H_U W] &= \bigoplus_{\chi \in X, \ker \chi = U} \text{Ind}^G(\chi \otimes \mathbf{1}_{H_\chi}) \quad \text{for } U \in \mathcal{U}. \end{aligned}$$

To do this, first compute the decomposition of  $\mathbb{C}[G/T]$  into irreducible characters for an arbitrary  $T < G$ . The multiplicity  $m_{\chi, \rho}^T$  of  $\text{Ind}^G(\chi \otimes \rho)$  in  $\mathbb{C}[G/T]$  is

$$\begin{aligned} m_{\chi, \rho}^T &= \langle \text{Ind}_{S_\chi}^G(\chi \otimes \rho), \text{Ind}^G \mathbf{1}_T \rangle_G = \langle \text{Res}_T \text{Ind}_{S_\chi}^G(\chi \otimes \rho), \mathbf{1} \rangle_T \\ &= \sum_{x \in S_\chi \backslash G/T} \langle \text{Ind}^{T^x} \text{Res}_{S_\chi \cap T^x}(\chi \otimes \rho), \mathbf{1} \rangle_{T^x} \\ &= \sum_{x \in S_\chi \backslash G/T} \langle \text{Res}_{S_\chi \cap T^x}(\chi \otimes \rho), \mathbf{1} \rangle_{S_\chi \cap T^x}. \end{aligned}$$

Next, take  $T = H$ . Since  $W \subseteq S_\chi$  for each  $\chi \in X$ , there is a unique double coset in  $S_\chi \backslash G/H$ , the trivial one. So

$$m_{\chi, \rho}^H = \langle \text{Res}_{H_\chi}(\chi \otimes \rho), \mathbf{1}_{H_\chi} \rangle_{H_\chi} = \langle \rho, \mathbf{1}_{H_\chi} \rangle_{H_\chi} = \begin{cases} 1, & \rho = \mathbf{1} \\ 0, & \rho \neq \mathbf{1}, \end{cases}$$



as claimed. Finally, for  $U \in \mathcal{U}$  we compare  $m_{\chi, \rho}^{H_U U}$  and  $m_{\chi, \rho}^{H_U W}$ .

If  $\chi = \mathbf{1}$  and  $\rho$  is an irreducible representation of  $G/W$  lifted to  $G$ , then

$$\begin{aligned} m_{\chi, \rho}^{H_U U} &= \langle \text{Ind}^G \mathbf{1}_{H_U U}, \rho \rangle_G = \langle \mathbf{1}, \text{Res}_{H_U U} \rho \rangle_{H_U U} \\ &= \langle \mathbf{1}, \text{Res}_{H_U} \rho \rangle_{H_U} = \langle \text{Ind}^G \mathbf{1}_{H_U W}, \rho \rangle_G = m_{\chi, \rho}^{H_U W}. \end{aligned}$$

For  $\chi \neq \mathbf{1}$ ,

$$m_{\chi, \rho}^{H_U U} = \sum_{x \in S_\chi \backslash G / H_U U} \langle \text{Res}_{S_\chi \cap (H_U U)^x} (\chi \otimes \rho), \mathbf{1} \rangle_{S_\chi \cap (H_U U)^x}.$$

If  $\ker \chi \neq U$  or, if  $\ker \chi = U$  but  $x$  represents a non-trivial double coset, then the corresponding summand is 0 since each  $S_\chi \cap (H_U U)^x$  contains a hyperplane of  $W$  distinct from  $\ker \chi$  and the restriction to this hyperplane is a sum of several copies of one non-trivial character. The same is true for  $H_U W$ . On the other hand, if  $\ker \chi = U$ , then

$$m_{\chi, \rho}^{H_U U} = \begin{cases} 1, & \rho = \mathbf{1} \\ 0, & \rho \neq \mathbf{1} \end{cases} \quad \text{and} \quad m_{\chi, \rho}^{H_U W} = 0.$$

□

**Proposition 6.5.** *Let  $G = C_l \rtimes H$ , with  $l$  prime and  $H \neq \{1\}$  acting faithfully on  $C_l$ . Then  $\text{Prim}(G) \cong \mathbb{Z}$ . If  $H \cong C_{p^k}$  is of prime-power order, then  $\text{Prim}(G)$  is generated by*

$$C_{p^{k-1}} - pH - C_l \rtimes C_{p^{k-1}} + pG.$$

*If  $H \cong C_{mn}$  with coprime  $m, n > 1$ , then  $\text{Prim}(G)$  is generated by*

$$G - H + \alpha(C_n - C_l \rtimes C_n) + \beta(C_m - C_l \rtimes C_m),$$

*where  $\alpha m + \beta n = 1$ .*

*Proof.* The existence of the two relations follows immediately from Example 2.3, applied to  $\tilde{H} = C_m < H$  and  $\tilde{H} = C_n < H$ . If  $H$  has composite order, the result follows from Theorem 4.3. If  $H \cong C_{p^k}$ , then  $G$  is  $p$ -quasi-elementary, so the coefficient of  $G$  in any relation is divisible by  $p$  by Theorem 4.2. Clearly, no relation in which  $G$  enters with non-zero coefficient can be induced from a subgroup. But also, no such relation can be lifted from a proper quotient, since all proper quotients of  $G$  are cyclic and therefore have no non-trivial relations. □

**Corollary 6.6.** *Theorem A holds for all finite non-quasi-elementary groups.*

*Proof.* The theorem is already proved for non-soluble groups (Remark 4.7), so suppose  $G$  is soluble but not quasi-elementary. Then, if  $G$  has a primitive relation, it falls under (ii) or (iii) of Theorem 6.1. This gives one direction.

Conversely, suppose  $G$  is of one of these two types, in particular  $G \cong (C_l)^d \rtimes Q$ , with  $Q$  quasi-elementary and acting faithfully on  $(C_l)^d$  by conjugation. It is easy to see that every proper quotient of  $G$  is quasi-elementary. So Theorem 4.3 combined with Proposition 6.4 for  $d \geq 2$  and Proposition 6.5 for  $d = 1$  give the asserted description of  $\text{Prim}(G)$ . □

## 7. QUASI-ELEMENTARY GROUPS

In the rest of the paper, we determine the structure and the representatives of  $\text{Prim}(G)$  for quasi-elementary groups that are not  $p$ -groups. This is case (2) of Theorem A, and it is by far the most difficult one.

**Notation 7.1.** Throughout the section,  $G = C \rtimes P$  is  $p$ -quasi-elementary, so  $P$  is a  $p$ -group and  $C$  is cyclic of order coprime to  $p$ . We assume  $C \neq \{1\}$  and we will denote by  $K \triangleleft P$  the kernel of the action of  $P$  on  $C$ .

We begin by showing that the presence of primitive relations forces tight restrictions on the structure of  $K$ . We then write down generators for  $\text{Prim}(G)$  and give necessary and sufficient group-theoretic criteria for these relations to be primitive.

## 7.1. The kernel of the conjugation action.

**Lemma 7.2.** *If  $P$  has normal  $p$ -rank one or is isomorphic to  $D_8$ , and  $K \neq \{1\}$ , then  $G$  has no primitive relations.*

*Proof.* We may assume that  $P \not\cong C_p$ , for otherwise  $K = P$  and  $G = P \times C$  is cyclic. We will consider the four possibilities for  $P$  separately (cf. Proposition 5.2). Denote by  $C_p^z$  the unique central subgroup of  $P$  of order  $p$ . Note that  $K$  contains  $C_p^z$ , since any normal subgroup of a  $p$ -group intersects its centre non-trivially.

If  $P$  is *cyclic or generalised quaternion*, then every non-trivial subgroup of  $P$  contains  $C_p^z$ . So every subgroup of  $G$  either contains  $C_p^z$ , or contains a non-trivial subgroup of  $C$ , or is contained in  $D = C_p^z \times C \triangleleft G$ . By Corollary 3.8,  $G$  has no primitive relations.

If  $P$  is *semi-dihedral*, then there is only one conjugacy class of subgroups of  $P$  that do not contain  $C_2^z$ , represented by  $\langle x \rangle$ . Now, up to conjugation, every subgroup of  $G$  either contains  $C_2^z$  or a non-trivial subgroup of  $C$ , or is contained in  $D = C \rtimes (C_2^z \times \langle x \rangle) \triangleleft G$ . By Corollary 3.8, we are done.

If  $P$  is *dihedral*, then there are two conjugacy classes of non-trivial subgroups of  $P$  that intersect  $\langle c \rangle$  trivially,  $I$  and  $J$ , say. They are each generated by a non-central involution. There is a  $P$ -relation

$$I - J - IC_2^z + JC_2^z.$$

Thus, any occurrence of  $I$  in any relation can be replaced by groups that either contain  $J$  or are contained in  $JC_2^z$ , using a relation that is induced from  $P$ , which is a proper subgroup of  $G$ . Similarly, any occurrence of  $\tilde{C} \rtimes I$  for  $\tilde{C} \leq C$  can be replaced by subgroups that either contain  $J$  or are contained in  $C \rtimes JC_2^z$  using a relation from a proper subquotient. In summary, by adding imprimitive relations to any given  $G$ -relation, all subgroups can be arranged to either contain  $C_2^z$  or be contained in  $C \rtimes JC_2^z$  and we are again done by Corollary 3.8.  $\square$

**Lemma 7.3.** *Suppose  $P$  has a non-central normal subgroup  $E \cong C_p \times C_p$  that meets  $K$  non-trivially. Then  $G$  has no primitive relations.*

*Proof.* Since  $E \triangleleft P$ , the intersection  $U = E \cap Z(P)$  is non-trivial. By assumption,  $U$  is not the whole of  $E$ , so  $C_p \cong U \triangleleft P$  and the action of  $P$  on  $E$  by conjugation factors through a group  $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$  of order  $p$ . In particular, no

other  $C_p < E$  except for  $U$  is normal in  $P$ , so every normal subgroup of  $P$  that meets  $E$  non-trivially must contain  $U$ ; hence  $U \subset K$ . So  $U$  commutes both with  $C$  and with  $P$ , in particular  $U \triangleleft G$ .

The centraliser  $C_P(E)$  of  $E$  in  $P$  has index  $p$  in  $P$ . By [11, Lemma 6.15], if  $H$  is any subgroup of  $P$  that does not contain  $U$  and is not contained in  $C_P(E)$ , then any occurrence of  $H$  in a relation can be replaced by subgroups that either contain  $U \leq Z(G)$  or are contained in  $C_P(E)$  using a relation induced from  $P$ , which is a proper subgroup of  $G$ . Similarly, any group of the form  $\tilde{C} \rtimes H$  for  $\tilde{C} \leq C$  and  $H$  as above can be replaced by subgroups that either contain  $U$  or are contained in  $D = C \rtimes C_P(E)$  using a relation from the quotient  $G/\tilde{C}$ . By Corollary 3.8,  $G$  has no primitive relations.  $\square$

**Corollary 7.4.** *If  $K \neq \{1\}$  and  $P$  has cyclic centre, then  $G$  has no primitive relations.*

*Proof.* If  $P$  has normal  $p$ -rank one, we are done by Lemma 7.2. Otherwise  $P$  has a normal subgroup  $E \cong C_p \times C_p$  (cf. proof of 5.3). Since  $Z(P)$  is cyclic,  $E$  is not central. Also, both  $E$  and  $K$  meet  $Z(P)$ , so they both contain the unique  $C_p < Z(P)$ , and thus  $G$  has no primitive relations by Lemma 7.3.  $\square$

**Lemma 7.5.** *Let  $T$  be any  $p$ -group. Then either  $T = \{1\}$  or  $T \cong D_8$  or  $T$  has normal  $p$ -rank one or the number of normal subgroups of  $T$  isomorphic to  $C_p \times C_p$  is congruent to 1 modulo  $p$ .*

*Proof.* By a Theorem of Herzog [21, Theorem 3], the number  $\alpha$  of elements in  $T$  of order  $p$  is congruent to  $-1$  modulo  $p^2$  if and only if  $T \neq D_8$  and has normal  $p$ -rank greater than one. We consider two cases:

**Case 1:**  $Z(T)$  is cyclic. Since every normal subgroup of  $T$  intersects the centre non-trivially and since there is a unique subgroup  $\langle z \rangle$  of order  $p$  in the centre, any normal  $C_p \times C_p$  is generated by  $z$  and a non-central element  $a$  of order  $p$ . For an arbitrary non-central element  $a$  of order  $p$ ,  $\langle a, z \rangle$  need not be normal, but the size of its orbit under conjugation is a power of  $p$ . So the number of normal such  $C_p \times C_p$  is congruent modulo  $p$  to the number of all  $C_p \times C_p$  that intersect the centre non-trivially. Finally,  $p^2 - p$  different non-central elements generate the same subgroup, so the number  $\beta$  of normal subgroups isomorphic to  $C_p \times C_p$  is congruent to  $(\alpha - (p - 1))/(p^2 - p)$  modulo  $p$ . Thus,

$$\begin{aligned} T \neq D_8 \text{ and } \exists C_p \times C_p \triangleleft T &\Leftrightarrow \alpha \equiv -1 \pmod{p^2} \\ &\Leftrightarrow \alpha - p + 1 \equiv -p \pmod{p^2} \\ &\Leftrightarrow \beta = \frac{\alpha - (p-1)}{p^2 - p} \equiv 1 \pmod{p}, \end{aligned}$$

as required.

**Case 2:**  $Z(T)$  is not cyclic. Then a normal subgroup of  $T$  isomorphic to  $C_p \times C_p$  is either contained in  $Z(T)$  or intersects it in a line. Let  $Z(T)$  have normal  $p$ -rank  $r \geq 2$ . Any  $C_p \times C_p \leq Z(T)$  is generated by two linearly independent elements of order  $p$  and there are  $(p^r - 1)(p^r - p)/2$  unordered pairs of such elements. Each  $C_p \times C_p$  contains  $(p^2 - 1)(p^2 - p)/2$  pairs and so there are

$$\frac{(p^r - 1)(p^r - p)}{(p^2 - 1)(p^2 - p)} = \frac{(p^r - 1)(p^{r-1} - 1)}{(p^2 - 1)(p - 1)} \equiv 1 \pmod{p}$$

distinct subgroups of  $Z(T)$  that are isomorphic to  $C_p \times C_p$ . Since there are  $p^r - 1 \equiv -1 \pmod{p^2}$  elements in  $Z(T)$  of order  $p$ , we have by Herzog's theorem that

$$T \neq D_8 \text{ and } \exists C_p \times C_p \triangleleft T \Leftrightarrow \#\{g \in T \setminus Z(T) \mid g^p = 1\} \equiv 0 \pmod{p^2}.$$

For any given line in  $Z(T)$ , the number of  $C_p \times C_p \leq T$  intersecting  $Z(T)$  in that line is therefore divisible by  $p$  by the same counting as above and so the number of normal  $C_p \times C_p$  in  $T$  that intersect  $T$  in a line is divisible by  $p$ , as required.  $\square$

**Proposition 7.6.** *Suppose that  $G$  has a primitive relation. Then either  $K = \{1\}$  or  $K \cong D_8$  or  $K$  has normal  $p$ -rank one. In particular,  $K$  has cyclic centre.*

*Proof.* If  $K$  is not of these three types, then by Lemma 7.5, the set of normal  $C_p \times C_p$  in  $K$  has cardinality coprime to  $p$ . The  $p$ -group  $P$  acts on this set by conjugation, so there is a fixed point. In other words, there is  $N = C_p \times C_p \triangleleft K$  that is fixed under conjugation by  $P$ , so  $N \triangleleft P$ . Now, either  $N$  is in the centre of  $P$ , in which case it is also in the centre of  $G$  (since  $K$  commutes with  $C$  by definition) and  $G$  has no primitive relations by Lemma 3.2; or  $N$  is a normal non-central subgroup of  $P$  that meets  $K$ , and then  $G$  has no primitive relations by Lemma 7.3.  $\square$

**Lemma 7.7.** *If  $C_{l^2} \leq C$  for some prime  $l$ , then  $G$  has no primitive relations.*

*Proof.* Write  $C \cong C_{l^n} \times \tilde{C}$  with  $\tilde{C}$  cyclic of order prime to  $l$ . There is a unique subgroup  $U$  of  $C$  isomorphic to  $C_l$ . Any subgroup of  $G$  that does not contain  $U$  is contained in  $\tilde{C} \rtimes P$  and, a fortiori, in  $D = (U \times \tilde{C}) \rtimes P \leq G$ . Since  $U \triangleleft G$ , we are done by Corollary 3.8.  $\square$

**Notation 7.8.** From now on, assume that  $C = C_{l_1} \times \dots \times C_{l_t}$ , where  $l_j$  are distinct primes. Assume also that  $K$  is as in Proposition 7.6. Whenever  $K$  is non-trivial, denote by  $C_p^z$  the unique central subgroup of  $K$  of order  $p$ .

**Notation 7.9.** If  $K \not\cong Q_8$  is non-trivial, then it contains a unique cyclic subgroup of index  $p$ , which is normal in  $G$ . In  $Q_8$ , there are three cyclic subgroups of index 2 and the 2-group  $P$  acts on them by conjugation, so this action has a fixed point, which is also normal in  $G$ . A subgroup of  $G$  intersects such a cyclic subgroup if and only if it contains  $C_p^z$ . Let  $C_K$  be either  $K$  if  $K$  is cyclic, or a cyclic index 2 subgroup of  $K$  that is normal in  $G$  otherwise. Then  $\bar{C}_K = CC_K$  is a normal cyclic subgroup of  $G$ , and  $G$  is an extension of the form

$$1 \rightarrow \bar{C}_K \rightarrow G \rightarrow \bar{P} \rightarrow 1,$$

where  $\bar{P}$  acts faithfully on  $\bar{C}_K$ .

Any relation in which every term contains a subgroup of  $\bar{C}_K$  is imprimitive by Lemma 3.1. So, to find generators of  $\text{Prim}(G)$ , we will from now on focus on relations that contain subgroups of  $P$  (since all Sylow  $p$ -subgroups of  $G$  are conjugate, we may fix one of them and work inside that) not containing  $C_p^z$ , or equivalently, subgroups of  $G$  that intersect  $\bar{C}_K$  trivially.

## 7.2. A generating set of relations.

**Notation 7.10.** Denote the set of subgroups of  $G$  that intersect  $\bar{C}_K$  trivially by  $\mathcal{H}$ . For elements  $\Theta_1 = \sum_H n_H H$  and  $\Theta_2 = \sum_H m_H H$  of the Burnside ring of  $G$ , write  $\Theta_1 \equiv \Theta_2 \pmod{\bar{C}_K}$  if  $n_H = m_H$  for all  $H \leq \bar{C}_K$ .

**Lemma 7.11.** *Let  $H \in \mathcal{H}$  and let  $\phi$  be a faithful irreducible character of  $\bar{C}_K$ . Then  $\text{Ind}_{\bar{C}_K}^G \phi$  is irreducible and any irreducible character of  $G$  whose restriction to  $\bar{C}_K$  is faithful is of this form. Moreover,*

$$\langle \mathbb{C}[G/H], \text{Ind}_{\bar{C}_K}^G \phi \rangle = \frac{|\bar{P}|}{|H|}.$$

*Proof.* Since  $\bar{P} = G/\bar{C}_K$  acts faithfully on  $\bar{C}_K$ , it also acts faithfully on the faithful characters of  $\bar{C}_K$ , so by Mackey's formula,

$$\langle \text{Ind}_{\bar{C}_K}^G \phi, \text{Ind}_{\bar{C}_K}^G \phi \rangle = \langle \phi, \text{Res}_{\bar{C}_K}^G \text{Ind}_{\bar{C}_K}^G \phi \rangle = \sum_{g \in \bar{C}_K \backslash G/\bar{C}_K} \langle \phi, \phi^g \rangle = 1,$$

i.e.  $\text{Ind}_{\bar{C}_K}^G \phi$  is irreducible. Moreover, if  $\chi$  is any irreducible character of  $G$  whose restriction to  $\bar{C}_K$  is faithful, then by Clifford theory, all irreducible summands of  $\text{Res}_{\bar{C}_K}^G \chi$  lie in one orbit under the action of  $G$ . Since any normal subgroup of  $\bar{C}_K$  is characteristic, all  $G$ -conjugate irreducible characters of  $\bar{C}_K$  have the same kernel, so all irreducible summands of  $\text{Res}_{\bar{C}_K}^G \chi$  are faithful. Thus, if  $\phi$  is one of them, then  $\chi = \text{Ind}_{\bar{C}_K}^G \phi$  by Frobenius reciprocity and by the first part of the lemma.

The rest of the lemma now follows by Mackey's formula:

$$\begin{aligned} \langle \text{Ind}_H^G \mathbf{1}, \text{Ind}_{\bar{C}_K}^G \phi \rangle &= \langle \mathbf{1}, \text{Res}_H \text{Ind}_{\bar{C}_K}^G \phi \rangle \\ &= \langle \mathbf{1}, \sum_{x \in H \backslash G/\bar{C}_K} \text{Ind}_{\bar{C}_K \cap H^x}^H \text{Res}_{\bar{C}_K \cap H^x} \phi^x \rangle \\ &= \sum_{x \in H \backslash G/\bar{C}_K} \langle \mathbf{1}, \text{Ind}_{\{1\}}^H \text{Res}_{\{1\}} \phi^x \rangle \\ &= \sum_{x \in H \backslash G/\bar{C}_K} \langle \mathbf{1}, \text{Ind}_{\{1\}}^H \mathbf{1} \rangle = |H \backslash G/\bar{C}_K| = \frac{|\bar{P}|}{|H|}. \end{aligned}$$

□

**Proposition 7.12.** *Let  $H_i \in \mathcal{H}$  and  $n_i \in \mathbb{Z}$ . Define  $\Theta_0 = \sum n_i H_i \in B(G)$  and, for  $1 \leq j \leq t$ , define  $\Theta_j = \Theta_{j-1} - C_{l_j} \Theta_{j-1}$ . Define  $\Theta_{t+1} = \Theta_t$  if  $K$  is trivial and  $\Theta_{t+1} = \Theta_t - C_p^z \Theta_t$  otherwise. In other words,*

$$\Theta_{t+1} = \sum_i n_i \sum_{U \leq \bar{C}_K} \mu(|U|) H_i U,$$

where  $\mu$  denotes the Moebius function and the inner sum runs over all subgroups of  $\bar{C}_K$ . Then, the following are equivalent:

- (1)  $\Theta_{t+1}$  is a relation;
- (2)  $\sum \frac{n_i}{|H_i|} = 0$ ;
- (3) there exists a relation of the form  $\Theta \equiv \sum_i n_i H_i \pmod{\bar{C}_K}$ .

*Proof.* Clearly, (1) implies (3). The implication (3)  $\Rightarrow$  (2) follows from the above lemma, by noting that if  $\phi = \text{Ind}_{\bar{C}_K}^G \chi$  is an irreducible character of  $G$

with faithful restriction to  $\bar{C}_K$ , then for all  $U$  intersecting  $\bar{C}_K$  non-trivially, we have

$$\langle \phi, \text{Ind}_U^G \mathbf{1}_U \rangle = \langle \chi, \text{Res}_{\bar{C}_K} \text{Ind}_U^G \mathbf{1}_U \rangle = \sum_{g \in \bar{C}_K \backslash G/U} \langle \text{Res}_{U^g \cap \bar{C}_K} \chi, \mathbf{1}_{U^g \cap \bar{C}_K} \rangle = 0.$$

Finally, to prove that (2) implies (1), we need to show that all irreducible characters vanish in the image of  $\Theta_{t+1}$  under  $B(G) \rightarrow R_{\mathbb{Q}}(G)$ . By the previous lemma and by the above calculation, this is true for those characters whose restriction to  $\bar{C}_K$  is faithful. So, let  $\rho$  be an irreducible character of  $G$  with  $C_l \leq \ker \rho$ , for some  $C_l = C_{l_j}$  or  $C_l = C_p^z$ . Then, for any  $H \leq G$ ,

$$\langle \rho, \text{Ind}_H^G \mathbf{1} \rangle = \langle \text{Res}_H^G \rho, \mathbf{1}_H \rangle = \langle \text{Res}_{HC_l}^G \rho, \mathbf{1}_{HC_l} \rangle = \langle \rho, \text{Ind}_{HC_l}^G \mathbf{1} \rangle,$$

so the contribution of such a  $\rho$  vanishes in  $\Theta_{t+1}$ , as required.  $\square$

**Corollary 7.13.** *Let  $H, H' \in \mathcal{H}$ .*

- (1) *If  $|H| = |H'|$ , then there is a relation  $\Theta \equiv H - H' \pmod{\bar{C}_K}$ .*
- (2) *If  $|H'| = p|H|$ , then there is a relation  $\Theta \equiv H - pH' \pmod{\bar{C}_K}$ .*

**Notation 7.14.** For  $1 \leq j \leq t$ , write  $C^j = C_{l_1} \times \dots \times \widehat{C_{l_j}} \times \dots \times C_{l_t}$  for the  $l'_j$ -Hall subgroup of  $C$ , and

$$K_j = \ker(P \rightarrow \text{Aut}(C^j)) = \bigcap_{i \neq j} \ker(P \rightarrow \text{Aut } C_{l_i}).$$

Thus  $K \leq K_j$  and  $K_j/K$  is cyclic, as it injects into  $\text{Aut } C_{l_j}$ .

**Lemma 7.15.** *Suppose that  $t > 1$ . For  $1 \leq j \leq t$ , write  $\tilde{K}_j = K_j \cap \ker(P \rightarrow \text{Aut } C_K)$ . Let  $H, H' \in \mathcal{H}$  be of maximal size among the elements of  $\mathcal{H}$  and suppose that  $HH' = P$ . If  $H \cap \tilde{K}_j = H' \cap \tilde{K}_j$  for some  $j$ , then there exists an imprimitive relation  $\Theta \equiv H - H' \pmod{\bar{C}_K}$ . Conversely, if there exists such a relation  $\Theta \equiv H - H' \pmod{\bar{C}_K}$  with the property that no term contains  $C_j$  (i.e. a relation of that form induced from  $C^j \rtimes P$ ), then  $H \cap \tilde{K}_j = H' \cap \tilde{K}_j$ .*

*Proof.* First, note that  $\tilde{K}_j$  is an extension of a cyclic group by  $C_K$  and the quotient acts trivially on  $C_K$ , so  $\tilde{K}_j$  is abelian and its Frattini quotient is of rank at most 2.

Suppose first that  $H \cap \tilde{K}_j = H' \cap \tilde{K}_j = N$ . Note, that  $N$  is normal in  $H$  and in  $H'$ , and therefore in  $HH' = P$ . Moreover, it acts trivially on  $C^j$ , so it is normal in  $C^j \rtimes P$ . We will lift a relation from  $C^j \rtimes P/N$ . If  $\tilde{K}_j/N$  is cyclic, then  $C^j \rtimes P/N$  is of the same type as  $G$  itself (see Notation 7.8), and we are done by inducing the relation of Proposition 7.12 from this subquotient. For the rest of the proof, assume that  $\tilde{K}_j/N$  is not cyclic, so it contains a subgroup  $E$  isomorphic to  $C_p \times C_p$ . Since  $\tilde{K}_j/N$  is abelian with two-dimensional Frattini quotient,  $E$  is characteristic, and hence normal in  $P/N$ . If this subgroup is central, then any order  $p$  subgroup of  $E$  that is not equal to  $NC_p^z/N$  generates together with  $H/N$  a subgroup of  $P/N$  that does not contain  $C_p^z$ , so it can be lifted to a subgroup of  $P$  that is in  $\mathcal{H}$  and strictly bigger than  $H$ , contradicting the maximality of  $|H|$ . So, suppose that  $E \cong C_p \times C_p \leq \tilde{K}_j/N$  is not central, let  $C_{P/N}(E)$  be its centraliser

in  $P/N$ , which is of index  $p$  in  $P/N$ . By [11, Lemma 6.15], there exists a subgroup  $H_s/N \leq C_{P/N}(E)$  and a  $P$ -relation

$$\Theta_1 = H/N - H_s/N - HC_p^z/N + H_s H_s C_p^z/N,$$

and similarly  $\Theta'_1$  for  $H'$ . Lifting  $H_s/N$  and  $H'_s/N$  to subgroups  $H_s, H'_s$  of  $P$  and applying Proposition 7.12 to  $H_s - H'_s$ , we get a relation  $\Theta_2 \equiv H_s - H'_s \pmod{\bar{C}_K}$  that is imprimitive by 3.7, since  $H_s H'_s$  is contained in an index  $p$ -subgroup of  $P$ . Finally, identifying the relations  $\Theta_1, \Theta'_1$  with their inductions from  $C^j \rtimes P/N$  to  $G$ , the relation  $\Theta = \Theta_1 - \Theta'_1 + \Theta_2 \equiv H - H' \pmod{\bar{C}_K}$  is the required imprimitive relation.

Conversely, suppose that  $H \cap \tilde{K}_j \neq H' \cap \tilde{K}_j$ . In particular,  $\tilde{K}_j$  is not cyclic. Without loss of generality (swapping  $H$  and  $H'$  if necessary), let  $\phi$  be a one-dimensional character of  $\tilde{K}_j$  that is trivial on  $H \cap \tilde{K}_j$  but non-trivial on  $H' \cap \tilde{K}_j$  and on  $C_p^z$ . Let  $\chi$  be a character of  $C$  with kernel  $C_{l_j}$ , extend it to a character of  $C \rtimes K_j$ , as in Remark 6.3. Let  $\rho = \text{Ind}_{C \rtimes K_j}^G (\chi \otimes \text{Ind}_{\tilde{K}_j}^{K_j} \phi)$ . To show that there can be no relation  $\Theta \equiv H - H' \pmod{\bar{C}_K}$  in which no term contains  $C_{l_j}$ , it suffices to show that the inner product of  $\rho$  with the image of such an element of  $B(G)$  in the representation ring can never be zero (note that we do not need  $\rho$  to be irreducible). If  $U$  is any subgroup of  $G$ , then by Mackey decomposition and Frobenius reciprocity, we have

$$\begin{aligned} \langle \text{Ind}_U^G \mathbf{1}, \rho \rangle &= \langle \mathbf{1}_U, \text{Res}_U^G \text{Ind}_{C \rtimes K_j}^G (\chi \otimes \text{Ind}_{\tilde{K}_j}^{K_j} \phi) \rangle \\ &= \sum_{g \in (C \rtimes K_j) \backslash G/U} \langle \mathbf{1}_U, \text{Ind}_U^U \text{Res}_{(C \rtimes K_j) \cap U}^{C \rtimes K_j} (\chi \otimes \text{Ind}_{\tilde{K}_j}^{K_j} \phi)^g \rangle \\ &= \sum_{g \in (C \rtimes K_j) \backslash G/U} \langle \mathbf{1}, \text{Res}_{(C \rtimes K_j) \cap U}^{C \rtimes K_j} (\chi \otimes \text{Ind}_{\tilde{K}_j}^{K_j} \phi) \rangle. \end{aligned}$$

If  $U$  contains some  $C_{l_i}$  for  $i \neq j$ , then this last expression is 0, since the restriction of  $\chi \otimes \text{Ind}_{\tilde{K}_j}^{K_j} \phi$  to  $C_{l_i}$  is a sum of copies of  $\chi$ , which is an irreducible faithful character. Also, the inner product is zero whenever  $U$  contains  $C_p^z$ , since the restriction of  $\rho$  to  $C_p^z$  is equal to the restriction of  $\text{Ind}_{\tilde{K}_j}^{K_j} \phi$ , which, by the choice of  $\phi$ , is a sum of non-trivial one-dimensional characters. If  $U = H$  or  $U = H'$ , then  $(C \rtimes K_j) \cap U \leq K_j$  and the restriction of  $\chi \otimes \text{Ind}_{\tilde{K}_j}^{K_j} \phi$  to this intersection is just the restriction of  $\text{Ind}_{\tilde{K}_j}^{K_j} \phi$  (since  $\chi$  is one dimensional and is extended to act trivially on  $K_j$ ), so that

$$\begin{aligned} \langle \text{Ind}_U^G \mathbf{1}, \rho \rangle &= \sum_{(C \rtimes K_j) \backslash G/U} \langle \mathbf{1}_{K_j \cap U}, \text{Res}_{K_j \cap U}^{K_j} \text{Ind}_{\tilde{K}_j}^{K_j} \phi \rangle \\ &= \sum_{\substack{(C \rtimes K_j) \backslash G/U \\ (K_j \cap U) \backslash K_j / \tilde{K}_j}} \langle \mathbf{1}_{\tilde{K}_j \cap U}, \text{Res}_{\tilde{K}_j \cap U}^{\tilde{K}_j} \phi \rangle. \end{aligned}$$

Recall that  $\phi$  was chosen such that the last inner product is positive if  $U = H$  and 0 if  $U = H'$ . Thus, the contribution from  $\rho$  in an element of the Burnside ring of the form  $\Theta \equiv H - H' \pmod{\bar{C}_K}$  cannot vanish if no term contains  $C_{l_j}$  and in particular, such an element cannot be a relation.  $\square$

A very similar argument establishes the following stronger result in a special case:

**Proposition 7.16.** *Suppose that some  $K_{j_0}$  is cyclic and let  $\Theta \equiv \sum_{H \in \mathcal{H}} n_H H \pmod{\bar{C}_K}$  be a relation with the property that no term contains  $C_{l_{j_0}}$ . Then, for any  $p^i \leq |K_{j_0}|$ , we have*

$$\sum_{\substack{|H \cap K_{j_0}| \leq p^i \\ HK_{j_0} = P}} n_H \equiv 0 \pmod{p}.$$

*Proof.* Let  $\text{Ind}_{C \rtimes K_{j_0}}^G (\chi \otimes \varphi)$  be an irreducible character of  $G$ , where  $\chi$  is a one-dimensional character of  $C$  with kernel  $C_{l_{j_0}}$ , extended to  $C \rtimes K_{j_0}$ , and  $\varphi$  is an irreducible character of  $K_{j_0}$ . Its inner product with permutation representations corresponding to subgroups of  $G$  that contain a subgroup of  $C$  other than  $C_{l_{j_0}}$  is 0, while for any  $H \leq P$ ,

$$\langle \text{Ind}_H^G \mathbf{1}, \text{Ind}_{C \rtimes K_{j_0}}^G (\chi \otimes \varphi) \rangle = \#(K_{j_0} \setminus P/H) \cdot \langle \mathbf{1}_{H \cap K_{j_0}}, \text{Res}_{H \cap K_{j_0}}^{K_{j_0}} \varphi \rangle,$$

as can be immediately deduced from Frobenius reciprocity and Mackey's formula, as in the previous lemma. So by assumption on  $\Theta$ , we must have

$$\sum_{H \leq P} n_H \#(K_{j_0} \setminus P/H) \cdot \langle \mathbf{1}_{H \cap K_{j_0}}, \text{Res}_{H \cap K_{j_0}}^{K_{j_0}} \varphi \rangle = 0$$

for any 1-dimensional character  $\varphi$  of  $K_{j_0}$ . Note that  $\langle \mathbf{1}_{H \cap K_{j_0}}, \text{Res}_{H \cap K_{j_0}}^{K_{j_0}} \varphi \rangle$  is either 1 or 0, according as  $H \cap K_{j_0}$  does or does not contain the kernel of  $\varphi$ . Also,  $\#(K_{j_0} \setminus P/H)$  is 1 if and only if  $HK_{j_0} = P$  and is a power of  $p$  otherwise, since  $K_{j_0}$  is normal in  $P$ . The result now follows by considering the above equation modulo  $p$  for  $\varphi$  with increasing kernels.  $\square$

**Proposition 7.17.** *Suppose that  $G$  does not satisfy the following equivalent conditions:*

- (1)  $P/K$  is generated by exactly  $t$  elements;
- (2)  $K_j \supsetneq K$  for  $1 \leq j \leq t$ ;
- (3)  $P/K$  acts faithfully on  $C$  but does not act faithfully any maximal proper subgroups of  $C$ .

*Then,  $G$  has no primitive relations.*

*Proof.* Let  $j_0$  be such that  $K_{j_0} = K$ , or equivalently that  $P/K$  acts faithfully on  $C_0 = C_{l_1} \times \dots \times \widehat{C_{l_{j_0}}} \times \dots \times C_{l_t}$ . Then,  $G_0 = C_0 \rtimes P$  is a group of the form described by Proposition 7.12, so there exists a  $G$ -relation  $\Theta \equiv \sum n_i H_i \pmod{\bar{C}_K}$  if and only if there exists a  $G_0$ -relation  $\Theta \equiv \sum n_i H_i \pmod{C_p^z C_0}$ , which can then be induced to an imprimitive  $G$ -relation. So all occurrences of  $H \in \mathcal{H}$  in any  $G$ -relation can be replaced by groups intersecting  $\bar{C}_K$  using imprimitive relations, so  $G$  has no primitive relations.  $\square$

**7.3. Primitive relations with trivial  $K$ .** As before, we have  $G = C \rtimes P$ , where  $C$  is a cyclic group of order  $l_1 \cdots l_t$  for distinct primes  $l_i \neq p$ , and  $P$  is a  $p$ -group. Assume throughout this subsection that  $K = \{1\}$ , that is  $P$  acts faithfully on  $C$ . In particular,  $P$  is abelian and its  $p$ -torsion is an elementary abelian  $p$ -group of rank at most  $t$ .



If  $t = 1$ , then  $\text{Prim}(G)$  has been described in Proposition 6.5, so we assume for the rest of the subsection that  $t > 1$ . Define  $\mathcal{M}$  to be the set of all index  $p$  subgroups of  $P$ . For each  $M \in \mathcal{M}$ , define the signature of  $M$  to be the vector in  $\mathbb{F}_2^t$  whose  $j$ -th coordinate is 1 if  $K_j \subseteq M$  and 0 otherwise.

**Proposition 7.18.** *The following properties of  $G$  are equivalent:*

- (1) *All  $K_j = \bigcap_{i \neq j} \ker(P \rightarrow \text{Aut } C_{l_i})$  have the same, non-trivial image in the Frattini quotient  $P/\Phi(P)$  of  $P$ .*
- (2) *Each subgroup of  $P$  of index  $p$  contains either all  $K_j$  or none, and both cases occur. In other words, the set of signatures of elements of  $\mathcal{M}$  is  $\{(1, \dots, 1), (0, \dots, 0)\}$ .*

*Proof.* A subgroup  $K_j$  has trivial image in  $P/\Phi(P)$  if and only if it is contained in all maximal proper subgroups of  $P$  if and only if the signatures of all  $M \in \mathcal{M}$  have a 1 in the  $j$ -th coordinate. Moreover,  $K_1$  and  $K_2$  have different non-trivial images in the Frattini quotient if and only if there are two hyperplanes in  $P/\Phi(P)$  containing one but not the other if and only if there are two subgroups in  $\mathcal{M}$  with signatures  $(1, 0, \dots)$  and  $(0, 1, \dots)$ .  $\square$

**Theorem 7.19.** *The group  $G$  has a primitive relation if and only if  $G$  satisfies the equivalent conditions of Proposition 7.18. If it does, then  $\text{Prim}(G) \cong C_p$  and is generated by the relation*

$$\sum_{U \leq C} \mu(|U|)(MU - M'U),$$

where  $M, M' \in \mathcal{M}$  have signatures  $(1, \dots, 1)$  and  $(0, \dots, 0)$ , respectively.

The proof will proceed in several lemmata.

**Lemma 7.20.** *The group  $\text{Prim}(G)$  is generated by relations of the form  $\Theta \equiv M - M' \pmod{C}$ , for  $M, M' \in \mathcal{M}$ .*

*Proof.* If a relation contains no subgroup of  $P$ , then it is imprimitive by Lemma 3.1. Let  $\Theta = n_H H + \dots$  be any relation with  $H \leq P$  of index at least  $p^2$ . Let  $M \in \mathcal{M}$  contain  $H$ . Filter  $M$  by a chain of subgroups, each of index  $p$  in the previous, such that at each step, the image in some  $\text{Aut}(C_{l_j})$  decreases. By Proposition 7.12, we can replace  $H$  by a subgroup  $H'$  in this chain and by subgroups intersecting  $C$  non-trivially, adding the relation  $\Theta_{t+1}$  from the proposition. Moreover, the added relation is induced from a subgroup, since  $\langle H, H' \rangle \leq M < P$ . Thus, the represented coset in  $\text{Prim}(G)$  has not changed. Next, we claim that each subgroup in the chain can be replaced by its supergroup in the chain and by subgroups of  $C$ , using an imprimitive relation. Let  $H' \leq H$  be an index  $p$  subgroup such that  $\text{Im}(H \rightarrow \text{Aut } C_{l_j}) \neq \text{Im}(H' \rightarrow \text{Aut } C_{l_j})$  for some  $j$ . Then, the subgroup  $C_{l_j} \rtimes H / \ker(H \rightarrow \text{Aut } C_{l_j})$  is a group of the form discussed in Example 2.3, with  $H'$  corresponding to  $\tilde{H}$  in that example. Lifting the relation of that example from the quotient,  $H'$  can be replaced by  $H$ , as claimed. So, in summary, we can replace any  $H \leq P$  by elements of  $\mathcal{M}$  and subgroups intersecting  $C$  non-trivially, without changing the class in  $\text{Prim}(G)$ .

Also, by Proposition 7.12, the coefficient of  $P$  in any relation is divisible by  $p$ . So we can again use the relation of Example 2.3, induced from the subquotient  $C_{l_1} \rtimes P / K_1$  (by Proposition 7.17, we may assume that  $K_1 \neq P$ ).

We have thus shown that we can replace any subgroup of  $P$  by a subgroup in  $\mathcal{M}$ , without changing the class in  $\text{Prim}(G)$ . Finally, by using relations  $\Theta \equiv M - M' \pmod{C}$ , we can replace all subgroups in  $\mathcal{M}$  by one of them. But the coefficient of this one must be zero by Proposition 7.12, so the resulting relation is imprimitive. Thus,  $\text{Prim}(G)$  is generated by relations  $\Theta \equiv M - M' \pmod{C}$ , as claimed.  $\square$

**Lemma 7.21.** *Let  $\Theta$  be a relation of the form  $\Theta \equiv M - M' \pmod{C}$  with  $M, M' \in \mathcal{M}$ . Then its order in  $\text{Prim}(G)$  divides  $p$ .*

*Proof.* Any occurrence of  $pM$  in a relation can be replaced by a proper subgroup of  $M$  and groups intersecting  $C$ , using the relation from Example 2.3, and similarly for  $M'$ . Next, these strictly smaller groups can all be replaced by one group of the same size, as in the above Lemma, using imprimitive relations. The resulting relation must then be  $0 \pmod{C}$  by Proposition 7.12, and so imprimitive.  $\square$

**Lemma 7.22.** *If  $M, M' \in \mathcal{M}$  have signatures that agree in some entry, then there is an imprimitive relation  $\Theta \equiv M - M' \pmod{C}$ .*

*Proof.* Say the signatures agree in the  $j$ th entry. If the common entry is 1, then  $M \cap K_j = M' \cap K_j = K_j$ , and if it is 0, then the intersections are both equal to the unique index  $p$  subgroup of  $K_j$ . In either case, there is an imprimitive relation of the required form by Lemma 7.15.  $\square$

**Lemma 7.23.** *If  $M, M' \in \mathcal{M}$  have opposite signatures both of which contain 0 and 1, then there is an imprimitive relation  $\Theta \equiv M - M' \pmod{C}$ .*

*Proof.* Suppose without loss of generality, that the signatures of  $M$  and  $M'$  start  $(0, 1, \dots)$  and  $(1, 0, \dots)$ , respectively. In particular, there exists  $g \in K_1 \setminus M$  with  $\langle M, g \rangle = P$  and  $g^p \in M$  and  $h \in K_2 \setminus M'$  with  $\langle M', h \rangle = P$  and  $h^p \in M'$ . Since  $M \cap M'$  is of index  $p$  in  $M$  and in  $M'$ , and since  $M = \langle M \cap M', g \rangle$  and similarly for  $M'$ , the group  $\langle M \cap M', gh \rangle$  is in  $\mathcal{M}$  and contains neither  $K_1$  nor  $K_2$ , i.e. it has signature  $(0, 0, \dots)$ . Thus we get the required relation by applying the previous lemma twice.  $\square$

**Corollary 7.24.** *If there exists  $M \in \mathcal{M}$  whose signature contains 0 and 1, then  $\text{Prim}(G)$  is trivial. Otherwise,  $\text{Prim}(G)$  is generated by any  $\Theta \equiv M - M' \pmod{C}$  where  $M$  and  $M'$  have signatures  $(0, \dots, 0)$  and  $(1, \dots, 1)$ , respectively.*

To conclude the proof of Theorem 7.19, it remains to show:

**Lemma 7.25.** *Suppose that no element of  $\mathcal{M}$  has a signature in which both 0 and 1 occur. Let  $M, M' \in \mathcal{M}$  have signatures  $(0, \dots, 0)$  and  $(1, \dots, 1)$ , respectively, let  $\Theta \equiv M - M' \pmod{C}$  be a relation. Then  $\Theta$  is primitive.*

*Proof.* Assume for a contradiction that  $\Theta$  is a sum of relations that are induced and/or lifted from proper subquotients. Then, at least one summand must contain terms in  $\mathcal{M}$  with signature  $(0, \dots, 0)$  such that the sum of all coefficients of these terms is congruent to 1 modulo  $p$ . Moreover, by Proposition 7.12 (2), this relation must contain either a term in  $\mathcal{M}$  with signature  $(1, \dots, 1)$ , or  $P$ . Since no  $M \in \mathcal{M}$  contains a normal subgroup of  $G$ , this relation cannot be lifted from a proper quotient, so it must be induced from

a proper subgroup. Since two distinct groups in  $\mathcal{M}$  generate  $P$ , this proper subgroup must be of the form  $(C_{l_1} \times \dots \times \widehat{C_{l_{j_0}}} \times \dots \times C_{l_t}) \rtimes P$ . But then, by Proposition 7.16, the sum of the coefficients of  $M \in \mathcal{M}$  with signature  $(0, \dots, 0)$  is divisible by  $p$ , which is a contradiction.  $\square$

**7.4. Primitive relations with non-trivial  $K$ .** In this subsection, we consider  $G = C \rtimes P$ , where  $C$  is a cyclic group of order  $l_1 \cdots l_t$  for distinct primes  $l_i$  different from  $p$ ,  $P$  is a  $p$ -group and the natural map  $P \rightarrow \text{Aut } C$  has a non-trivial kernel,  $K$ . By Proposition 7.6, if  $G$  has a primitive relation, then  $K$  must be isomorphic to  $D_8$  or have normal  $p$ -rank one, so it is a group of the type described in Proposition 5.2. We will assume this throughout this subsection. Note that in particular, if  $p$  is odd, then  $K$  must be cyclic.

Recall that  $\mathcal{H}$  is the set of subgroups of  $P$  that do not contain  $C_p^z$ , the unique subgroup of  $K$  of order  $p$  that is central in  $G$ . If a relation  $\Theta$  is primitive, then it must contain at least one subgroup in  $\mathcal{H}$  by Lemma 3.1. Let  $\mathcal{H}_m$  be the set of elements of  $\mathcal{H}$  of maximal size.

**Lemma 7.26.** *The group  $\text{Prim}(G)$  is generated by relations of the form*

$$\Theta = \sum_{\tilde{C} \leq \bar{C}_K} \mu(|\tilde{C}|)(\tilde{C}H - \tilde{C}H'),$$

for  $H, H' \in \mathcal{H}_m$ .

*Proof.* If there are no elements of  $\mathcal{H}$  in a relation, then the relation is imprimitive by Lemma 3.1. Let  $\Theta$  be a relation in which a subgroup  $H \in \mathcal{H}$  occurs and suppose that  $H' \in \mathcal{H}$  is such that  $|H'| = p|H|$ . Then,  $I_H = \text{Im}(H \rightarrow \text{Aut } C) \neq \text{Im}(P \rightarrow \text{Aut } C)$ . Let  $B$  be an index  $p$  subgroup of  $\text{Im}(P \rightarrow \text{Aut } C)$  containing  $I_H$ . By intersecting  $H'$  with the pre-image of  $B$  in  $P$  if necessary, we can find an index  $p$  subgroup  $H_2$  in  $H'$  such that  $H$  and  $H_2$  generate a proper subgroup of  $P$ . Thus, the relation  $\sum_{\tilde{C} \leq \bar{C}_K} \mu(|\tilde{C}|)(\tilde{C}H - \tilde{C}H_2)$  of Proposition 7.12 is induced from a proper subgroup by Proposition 3.7, so that  $H$  can be replaced by  $H_2$  and by subgroups of  $\bar{C}_K$  without changing the class in  $\text{Prim}(G)$ . By inducing the relation of Example 2.4 from the subquotient  $H'C_p^z/H_2 \cong C_p \times C_p$  (note that  $H'$  is abelian and  $C_p^z$  is central, so  $H_2$  is indeed normal in the group generated by the two), we may replace  $H_2$  by strictly bigger groups in  $\mathcal{H}$  and by subgroups of  $P$  containing  $C_p^z$ . In summary, any class in  $\text{Prim}(G)$  is represented by a relation of the form  $\Theta \equiv \sum n_i H_i \pmod{\bar{C}_K}$  with  $H_i \in \mathcal{H}_m$ .

Since  $\sum_i n_i = 0$  by Proposition 7.12, the generators of  $\text{Prim}(G)$  are as claimed.  $\square$

**Lemma 7.27.** *The group  $\text{Prim}(G)$  is an elementary abelian  $p$ -group.*

*Proof.* It suffices to show that for any  $H, H' \in \mathcal{H}_m$ ,

$$\Theta = p \cdot \sum_{\tilde{C} \leq \bar{C}_K} \mu(|\tilde{C}|)(\tilde{C}H - \tilde{C}H')$$

is imprimitive. Let  $A$  be a subgroup of  $\text{Im}(P \rightarrow \text{Aut } C)$  of index  $p$  and such that for some  $j$ ,  $A \cap \text{Aut } C_{l_j} \neq \text{Im}(P \rightarrow \text{Aut } C_{l_j})$ . By intersecting  $H$  and  $H'$  with the pre-image of  $A$  in  $P$ , we may find subgroups  $H_A \leq H$  and  $H'_A \leq H'$  of index  $p$  whose image in  $\text{Aut } C$  lies in  $A$ , and in particular whose image

in  $\text{Aut } C_{l_j}$  is strictly smaller than that of  $H$  and of  $H'$ , respectively. By inducing the relation of Example 2.3, we may replace  $pH$  and  $pH'$  in  $\Theta$  by  $H_A$  and  $H'_A$ , respectively, and by groups containing  $C_{l_j}$ , without changing the class of  $\Theta$  in  $\text{Prim}(G)$ . Now, we can replace  $H_A$  by  $H'_A$  and by groups intersecting  $\bar{C}_K$ , using the relation of Proposition 7.12. Since  $H_A$  and  $H'_A$  together generate a proper subgroup of  $G$  (it is contained in the pre-image of  $A$  in  $P$ ), the class of  $\Theta$  in  $\text{Prim}(G)$  still hasn't changed. But now, the only element of  $\mathcal{H}$  appearing in  $\Theta$  is  $H'_A$ , so by Proposition 7.12, it must appear with coefficient 0 and the resulting relation is imprimitive by Lemma 3.1.  $\square$

It only remains to determine the rank of  $\text{Prim}(G)$ . We will first treat separately the case that  $K = C_p^z$  and  $P$  is a direct product of  $K$  by a group that acts faithfully on  $C$ . In this case, each  $K_j$  is a direct product of  $K$  by a cyclic group, so the image of each  $K_j$  in  $P/\Phi(P)$  is an elementary abelian  $p$ -group of rank at most 2.

**Proposition 7.28.** *Let  $K = C_p^z$  and let  $P$  be a direct product by  $K$ . If there exists  $K_j$  with one-dimensional image in  $P/\Phi(P)$  or if there exist  $K_{j_1}$  and  $K_{j_2}$  with distinct images in  $P/\Phi(P)$ , then  $\text{Prim}(G)$  is trivial. Otherwise,  $\text{Prim}(G) \cong \mathbb{F}_p^{p-2}$ .*

*Proof.* Let  $H = \langle a_1, \dots, a_r \rangle$  be a complement to  $K$  in  $P$ , where  $r$  is the number of distinct prime divisors of  $|C|$ . Write  $K = \langle c \rangle$ . Then, any other element of  $\mathcal{H}_m$  is of the form  $\langle c^{\delta_1} a_1, \dots, c^{\delta_r} a_r \rangle$ , where  $\delta_i \in \{0, \dots, p-1\}$ .

**Step 1.** Suppose that there exists  $K_j$  with one-dimensional image in  $P/\Phi(P)$ . Equivalently, the image of  $K_j$  in  $P/\Phi(P)$  is equal to that of  $K$ . Then, the intersection of  $K_j$  with any complement to  $K$  in  $P$  has trivial image in the Frattini quotient, and therefore only consists of  $p$ -th powers. From the explicit description of these complements, it follows that the intersections of any two complements  $H_1$  and  $H_2$  with  $K_j$  are equal, since taking  $p$ -th powers kills  $c$ . So by Lemma 7.15, there exists an imprimitive relation  $\Theta \equiv H_1 - H_2 \pmod{C}$ . Combined with Lemma 7.26, this implies that  $\text{Prim}(G)$  is generated by a relation of the form  $\Theta \equiv n_H H \pmod{C}$ . But by Proposition 7.12,  $n_H = 0$ , and so  $\text{Prim}(G)$  is trivial by Lemma 3.1.

**Step 2.** Suppose that

$$K_{j_1}^\Phi = \text{Im}(K_{j_1} \rightarrow P/\Phi(P)) \neq K_{j_2}^\Phi = \text{Im}(K_{j_2} \rightarrow P/\Phi(P)),$$

without loss of generality assume that both images are two-dimensional. Then, given any line  $L_1 \leq K_{j_1}^\Phi$ , and any line  $L_2 \leq K_{j_2}^\Phi$ , both not equal to the image of  $C_p^z$ , we can lift a hyperplane in  $P/\Phi(P)$  that intersect each  $K_{j_i}^\Phi$  in  $L_i$  for  $i = 1, 2$  to an index  $p$ -subgroup of  $P$  that intersects  $K$  trivially. Thus, given any two complements  $H_1$  and  $H_2$ , we can find  $H_3$  such that  $H_i \cap K_{j_i} = H_3 \cap K_{j_i}$  for  $i = 1, 2$ . Thus, there exist imprimitive relations  $\Theta_i \equiv H_i - H_3 \pmod{C}$  for  $i = 1, 2$  and so,  $\text{Prim}(G)$  is trivial by the same argument as in the previous step.

**Step 3.** For the rest of the proof, suppose that all images  $K_j^\Phi$  of  $K_j$  in the Frattini quotient of  $P$  are two-dimensional and all equal to some  $K^\Phi$ . Given any complement  $H'$  to  $K$  in  $P$ , the image of  $H' \cap K_j$  in  $P/\Phi(P)$  is a line, different from the image of  $C_p^z$ . Moreover, this line is the same for all  $j$ ,

since two different lines would generate the whole of  $K^\Phi$  and  $H'$  would then contain  $K$ . Let  $L_1, \dots, L_p$  be the distinct lines different from the image of  $K$  in  $K^\Phi$ . Consider the following map  $f : K(G) \rightarrow \mathbb{F}_p^p$ : given a relation  $\Theta \equiv \sum_{H_i \in \mathcal{H}} n_i H_i$  let  $f(\Theta)$  be the vector whose  $k$ -th entry is the sum of  $n_i$  modulo  $p$  over those  $i$  for which  $H_i \in \mathcal{H}_m$  and  $\text{Im}(H_i \cap K_j \rightarrow P/\Phi(P)) = L_k$ . The preceding discussion implies that any relation that is in the kernel of  $f$  is imprimitive. Indeed, if  $f(\Theta) = 0$ , then after adding the relations of Proposition 7.12 between groups in  $\mathcal{H}$  that have the same intersection with  $K_j$ , and relations of Example 2.3, we may assume that  $\Theta \equiv \sum_{k=1}^p n_k H_k \pmod{C}$  where  $p|n_k \forall k$  and  $H_k \cap K_j = L_k \forall j, k$ . The resulting relation is imprimitive by Lemma 7.27.

**Step 4.** By Proposition 7.12, the image of  $f$  is precisely equal to the hyperplane  $V = \{(v_1, \dots, v_p) \mid \sum v_i = 0 \in \mathbb{F}_p\}$  of  $\mathbb{F}_p^p$ . By Step 3,  $\text{Prim}(G)$  is isomorphic to the quotient of  $V$  by the image of the imprimitive relations under  $f$ . Let  $\Theta$  be imprimitive with non-trivial image under  $f$ , without loss of generality assume that it is primitive in its own subquotient. Since  $f(\Theta) \neq 0$  and since any two groups in  $\mathcal{H}_m$  generate all of  $P$ , this subquotient is either a  $p$ -group or of the form  $\tilde{C} \rtimes P$ , where  $\tilde{C}$  is a proper subgroup of  $C$ . So, assume that  $\Theta$  is as described by Theorem 5.3 or by Lemma 7.26. If it is the former, then the subquotient must be isomorphic to  $C_p \times C_p$ , since  $P$  is abelian, and then  $f(\Theta) = (a, \dots, a)$  for some  $a \in \mathbb{F}_p$ . If it is the latter, then by Lemma 7.15,  $\Theta \equiv H_1 - H_2 \pmod{C}$  such that  $H_1 \cap K_j = H_2 \cap K_j$  for some  $j$ . But then  $f(\Theta) = 0$ . In summary, the image of the imprimitive relations under  $f$  is a one-dimensional subspace of  $V$ , so  $\text{Prim}(G) \cong \mathbb{F}_p^{p-2}$ , as claimed.  $\square$

**Theorem 7.29.** *Assume that either  $|K| > p$ , or  $P$  is not a direct product by  $K$ . Let  $\mathcal{H}_m$  be the set of subgroups of  $P$  of maximal size among those that intersect the centre of  $K$  trivially. Define a graph  $\Gamma$  whose vertices are the elements of  $\mathcal{H}_m$  and with an edge between  $H, H' \in \mathcal{H}_m$  if one of the following applies:*

- (1) *the subgroup generated by  $H$  and  $H'$  is a proper subgroup of  $P$ ;*
- (2)  *$t > 1$  and there exists  $1 \leq j_0 \leq t$  such that  $H \cap \tilde{K}_{j_0} = H' \cap \tilde{K}_{j_0}$ , where  $\tilde{K}_{j_0} = K_{j_0} \cap \ker(P \rightarrow \text{Aut } C_K)$  (recall that  $C_K$  is a fixed maximal cyclic subgroup of  $K$  that is normal in  $G$ , see Notation 7.9);*
- (3) *the intersection  $H \cap H'$  is of index  $p$  in  $H$  and in  $H'$ , and  $HH'/H \cap H'$  is either dihedral, or the Heisenberg group of order  $p^3$ .*

*Let  $d$  be the number of connected components of  $\Gamma$ . Then  $\text{Prim}(G) \cong (C_p)^{d-1}$ , generated by relations  $\Theta = \sum_{\tilde{C} \leq \tilde{C}_K} \mu(|\tilde{C}|)(\tilde{C}H - \tilde{C}H')$  for  $H, H' \in \mathcal{H}_m$  corresponding to distinct connected components of the graph.*

*Proof.* The three conditions for when there is an edge between  $H$  and  $H' \in \mathcal{H}_m$  ensure that if  $H$  and  $H'$  lie in the same connected component of the graph  $\Gamma$ , then there is an imprimitive relation  $\Theta \equiv H - H' \pmod{\tilde{C}_K}$ , by using Proposition 3.7, Lemma 7.15, and by inducing the relations of Theorem 5.3, respectively.

For a subgroup  $H \in \mathcal{H}_m$  write  $[H]$  for the connected component of  $\Gamma$  that contains  $H$ . Note that since the conjugation action of  $P$  on its Frattini quotient is trivial, condition (1) ensures that  $[H] = [H^g]$  for any  $g \in G$ .

Therefore  $[\cdot]$  extends by linearity to a well-defined linear map  $B(G) \rightarrow \mathbb{F}_p^d$ , defining it to be 0 on the groups not in  $\mathcal{H}_m$ . We are interested in its restriction to the space of relations,

$$[\cdot] : K(G) \longrightarrow \mathbb{F}_p^d.$$

Its image is the hyperplane  $\{\mathbf{v} \mid \sum v_i = 0\}$  (Proposition 7.12) and all the relations in its kernel are imprimitive (Lemma 7.27). We need to show that, conversely, every imprimitive relation is in  $\ker[\cdot]$ , so that

$$[\cdot] : \text{Prim } G \longrightarrow \mathbb{F}_p^{d-1}$$

is an isomorphism of  $\mathbb{F}_p$ -vector spaces.

Suppose, on the contrary, that  $[\Theta] \neq 0$  and  $\Theta$  is imprimitive. So  $\Theta = \sum_i \Theta_i$ , where each  $\Theta_i$  comes from a proper subquotient of  $G$ . Without loss of generality, we may assume that each of these summands is primitive in its subquotient. Moreover, using Lemma 7.26 and Theorem 7.19, we may assume further that  $\Theta_i$  that are induced from  $p$ -groups are of the form described in Theorem 5.3, while  $\Theta_i$  that are induced/lifted from quasi-elementary subquotients that are not  $p$ -groups are as described by Proposition 7.12.

Because  $[\Theta] \neq 0$ , we must have  $[\Theta_i] \neq 0$  for some index  $i$ . The entries of  $[\Theta_i] \in \mathbb{F}_p^d$  sum up to 0, so there must be at least two non-zero entries. In particular,  $\Theta_i$  contains two terms  $H_1$  and  $H_2$  in  $\mathcal{H}_m$  that lie in different connected components of  $\Gamma$  and which appear in  $\Theta_i$  with non-zero coefficients modulo  $p$ . Since both  $H_i$  act faithfully on  $\bar{C}_K$ , their intersection does not contain any normal subgroup of  $G$ , so  $\Theta_i$  must be induced from a proper subgroup of  $G$ . Since  $H_1$  and  $H_2$  lie in different connected components of  $\Gamma$ , they generate all of  $P$ . So  $\Theta_i$  is either induced from  $P$  or from  $\tilde{C} \rtimes P$  for a proper non-trivial subgroup  $\tilde{C}$  of  $C$ .

If  $\Theta_i$  is induced from  $P$ , then it is induced from a subquotient of the form described in Theorem 5.3 and  $H_i$ ,  $i = 1, 2$  correspond to two groups of order  $p$  in that subquotient. If  $H_1 H_2 \neq P$  or if this subquotient is dihedral or a Heisenberg group of order  $p^3$ , then there is an edge between  $H_1$  and  $H_2$  - contradiction. Otherwise, the intersection has index  $p$  in  $H_1$  and in  $H_2$  and  $H_1 H_2 = P$ , so that  $|P| = p|H_1|$ , i.e.  $K = C_p^z$ . Moreover,  $P/H_1 \cap H_2 \cong C_p \times C_p$ , so  $P = C_p^z \times H_1$  and this case was excluded.

If, on the other hand,  $\Theta_i$  is induced from a subgroup of the form  $\tilde{C} \rtimes P$ , then, by Lemma 7.15,  $H_1$  and  $H_2$  have the same intersection with some  $\tilde{K}_j$  and there is an edge between them - contradiction.  $\square$

**Remark 7.30.** This completes the proof of Theorem A in the last remaining case, when  $G = C \rtimes P$  is quasi-elementary with  $P$  a  $p$ -group and  $C$  cyclic of order prime to  $p$ .

The conditions in Theorem A(4) that describe when such a  $G$  has primitive relations are group-theoretic, but they are rather intricate. In the special case that  $|C| = l \neq p$  is prime, they can be made completely explicit, and one can list all such  $G$  in terms of generators and relations. We refer the interested reader to [5], and just make one remark here.

Suppose that  $G$  has a primitive relation. By Proposition 7.6, the kernel  $K$  of the action of  $P$  on  $C$  by conjugation is  $\{1\}$ ,  $D_8$  or has normal  $p$ -rank

one. Suppose that  $\{1\} \neq K \neq P$  (cf. Example 2.3, Lemma 7.2). Write  $A$  for the image of  $P$  in  $\text{Aut } C$ . What makes the case  $|C| = l$  simpler is that in this case  $A$  is cyclic and the sequence

$$(7.31) \quad 1 \rightarrow K \rightarrow P \rightarrow A \rightarrow 1$$

must split; this makes  $P = K \rtimes A$  and  $G$  not hard to describe by generators and relations.

Indeed, suppose the sequence does not split. If  $K$  is cyclic or generalised quaternion, then all subgroups of  $K$  contain the central  $C_p^z$ , so, using the notation of section 7.4,  $\mathcal{H}$  consists of subgroups of  $P$  that do not intersect  $K$ . Since there is no subgroup  $H$  of  $P$  with  $H \cap K = \{1\}$  and surjecting onto  $A$  (otherwise  $P$  would be a semi-direct product of  $H$  by  $K$ ), all subgroups in  $\mathcal{H}$  must be contained in the pre-image under  $P \rightarrow \text{Aut } C$  of the unique index  $p$  subgroup. Thus, there is an edge between any two groups in  $\mathcal{H}_m$ , using the notation of Theorem 7.29, and so  $\text{Prim}(G) = \{1\}$ . Now suppose  $K$  is dihedral or semi-dihedral (the latter cannot actually occur), and denote by  $C_K$  the unique cyclic index 2 subgroup of  $K$ . Since the automorphism of  $C_K$  given by any non-central involution of  $K$  is not divisible,  $P$  not being a semi-direct product by  $K$  implies that it is not a semi-direct product by  $C_K$  either. Thus, again, there is an index  $p$  subgroup of  $P$  containing any subgroup of  $P$  that does not intersect  $C_K$ , so the same argument applies and shows that  $\text{Prim}(G) = \{1\}$ .

Finally, let us mention that when  $C$  has composite order, it may happen that the sequence (7.31) does not split, but  $G$  still has primitive relations. The smallest such example that we know is a group  $G$  of order  $3934208 = 2^{11} \cdot 17 \cdot 113$ , with  $C = C_{17} \times C_{113}$ ,  $K = C_8$  and  $A = C_{16} \times C_{16}$ .<sup>3</sup> Here there are no subgroups in  $\mathcal{H}$  mapping onto  $A$ , but the images of two elements of  $\mathcal{H}$  may generate the whole of  $A$  (this cannot happen when  $C$  has prime order).

## 8. EXAMPLES

**Example 8.1.** Let  $G = \text{SL}_2(\mathbb{F}_3)$ . Its Sylow 2-subgroup  $Q$  is normal in  $G$  and is isomorphic to the quaternion group  $Q_8$ . The Sylow 2-subgroup and  $G$  itself are the only non-cyclic subgroups of  $G$ , so  $K(G)$  has rank 2. Since  $G$  is not in the list of Theorem A, all its relations come from proper subquotients. By Theorem 5.3,  $K(Q)$  is generated by the relation lifted from  $Q/Z(Q) \cong C_2 \times C_2$ . The only other subquotient of  $G$  that has primitive relations is  $G/Z(G) \cong A_4$ , which is of type 3(a) in Theorem A with  $Q$  cyclic. Combining everything we have said and noting that the three cyclic subgroups of order 4 in  $Q$  are conjugate in  $G$ , we see that  $K(G)$  is generated by

$$\begin{aligned} \Theta_1 &= C_4 - C_6 - Q + G, \\ \Theta_2 &= C_2 - 3C_4 + 2Q. \end{aligned}$$

**Example 8.2.** Let  $G = A_5$ . Since  $G$  is simple, Theorem 4.3 shows that  $G$  has a primitive relation and  $\text{Prim}(G) \cong \mathbb{Z}$  and is generated by any relation in

<sup>3</sup> In Magma, this group may be given by  $\text{PolycyclicGroup}\langle a, b, c, d, e, f, g, h, i, j, k, l, m \mid a^2 = f, b^2 = e, c^2 = d, d^2 = h, e^2 = g, f^2 = i, g^2 = k, h^2 = j, i^2 = j^2 = k^2 = l^{17}, m^{113}, c^a = c \cdot i, c^b = c \cdot f, d^b = d \cdot i, e^c = e \cdot i, l^b = l^3, l^e = l^9, l^g = l^{13}, l^k = l^{16}, m^b = m^{48}, m^c = m^{42}, m^d = m^{69}, m^e = m^{44}, m^g = m^{15}, m^h = m^{15}, m^j = m^{112}, m^k = m^{112} \rangle$

which  $G$  enters with coefficient 1. Using [30, Theorem 2.16(i)] or explicitly decomposing all permutation characters in  $A_5$  into irreducible characters, we find that

$$\Theta = C_2 - C_3 - V_4 + S_3 - D_{10} + G$$

is a relation (of the form predicted by Theorem 4.1). Theorem 4.3 now implies that all Brauer relations in  $G$  can be expressed as integral linear combinations of  $\Theta$  and of relations coming from proper subgroups. The non-cyclic proper subgroups of  $G$  are  $V_4$ ,  $S_3$ ,  $D_{10}$  and  $A_4$  and their relations induced to  $G$  together with  $\Theta$  generate  $K(G)$ .

**Example 8.3.** Let  $G = C_3 \wr C_4$  be the wreath product of  $C_3$  by  $C_4$ . Then the subspace of  $\mathbb{F}_3^4$  on which  $C_4$  acts trivially is a normal subgroup of  $G$  with non-quasi-elementary quotient. Thus, all relations of  $G$  are obtained from proper subquotients by Corollary 4.4.

## 9. AN APPLICATION TO REGULATOR CONSTANTS

Let  $\Theta = \sum_H n_H H$  be a Brauer relation in a group  $G$ . Write

$$\mathcal{C}_\Theta(\mathbf{1}) = \prod_H |H|^{-n_H}.$$

This quantity is called the *regulator constant* of the trivial  $\mathbb{Z}G$ -module. We refer the reader to [15] §2.2 and [2] §2.2 for the definition of regulator constants for general  $\mathbb{Z}G$ -modules and their properties. Note that  $\mathcal{C}_\Theta(\mathbf{1})$  is invariant under induction of  $\Theta$  from subgroups and lifts from quotients (using  $\sum n_H = \langle \Theta, \mathbf{1} \rangle = 0$ ), and that  $\mathcal{C}_{\Theta+\Theta'}(\mathbf{1}) = \mathcal{C}_\Theta(\mathbf{1})\mathcal{C}_{\Theta'}(\mathbf{1})$ .

As an application of Theorem A, we classify, given a prime number  $l$ , all finite groups  $G$  that have a Brauer relation  $\Theta$  with the property that  $\text{ord}_l(\mathcal{C}_\Theta(\mathbf{1})) \neq 0$ . For an example of number theoretic consequences of the theorem, see [4].

**Theorem 9.1.** *Let  $G$  be a finite group and  $l$  a prime number. Then any Brauer relation  $\Theta$  in  $G$  is a sum of a relation  $\Theta'$  satisfying  $\text{ord}_l(\mathcal{C}_{\Theta'}(\mathbf{1})) = 0$  and relations from the following list, induced and/or lifted from subquotients  $H = \mathbb{F}_l^d \rtimes Q$  of the following form:*

- (1)  $d = 1$ ,  $Q = C_{p^{k+1}}$ ,  $p \neq l$  prime,  $Q$  acting faithfully on  $C_l$ ;  $\Theta = C_{p^k} - pQ - C_l \rtimes C_{p^k} + pH$ ;  $\mathcal{C}_\Theta(\mathbf{1}) = l^{-p+1}$ .
- (2)  $d = 1$ ,  $Q = C_{mn}$  acting faithfully on  $C_l$ ,  $(m, n) = 1$ ,  $m\alpha + n\beta = 1$ ;  $\Theta = H - Q + \alpha(C_n - \mathbb{F}_l \rtimes C_n) + \beta(C_m - \mathbb{F}_l \rtimes C_m)$ ;  $\mathcal{C}_\Theta(\mathbf{1}) = l^{\alpha+\beta-1}$ .
- (3)  $d > 1$ , either  $Q$  is quasi-elementary and acts faithfully irreducibly on  $(\mathbb{F}_l)^d$ , or  $H = (C_l \rtimes P_1) \times (C_l \rtimes P_2)$ , where  $P_1, P_2$  are cyclic  $p$ -groups,  $p \neq l$ , acting faithfully on the respective  $C_l$ ;

$$\Theta = H - Q + \sum_{U \in \mathcal{U}} \left( U \rtimes N_Q U - \mathbb{F}_l^d \rtimes N_Q U \right);$$

$\mathcal{C}_\Theta(\mathbf{1}) = l^{|\mathcal{U}|-d}$ , where  $\mathcal{U}$  is the set of index  $l$  subgroups of  $\mathbb{F}_l^d$  up to  $Q$ -conjugation.

**Corollary 9.2.** *A group  $G$  has a Brauer relation  $\Theta$  with  $\text{ord}_l(\mathcal{C}_\Theta(\mathbf{1})) \neq 0$  if and only if it has a subquotient isomorphic either to  $C_l \times C_l$  or to  $C_l \rtimes C_p$  with  $C_p$  of prime order acting faithfully on  $C_l$ .*



*Proof.* If  $G$  has a subquotient  $C_l \times C_l$ , respectively  $C_l \rtimes C_p$ , then the induction/lift of a relation from Example 2.4, respectively 2.3 is as required. The converse immediately follows from Theorem 9.1, noting that all groups listed there have a subquotient of the required type.  $\square$

We begin by reducing the theorem to soluble groups.

**Definition 9.3.** We call a Brauer relation  $\Theta = \sum_H H - \sum_{H'} H'$  in  $G$  a  $\mathbb{Z}_l$ -isomorphism if

$$\bigoplus_H \mathbb{Z}_l[G/H] \cong \bigoplus_{H'} \mathbb{Z}_l[G/H'],$$

or equivalently (see [7, Lemma 5.5.2]) if

$$\bigoplus_H \mathbb{F}_l[G/H] \cong \bigoplus_{H'} \mathbb{F}_l[G/H'].$$

The following result is a slight strengthening of [7, Theorem 5.6.11]:

**Theorem 9.4** (Dress's induction theorem). *Let  $G$  be a finite group and  $l$  a prime number. There exists a  $\mathbb{Z}_l$ -isomorphism in  $G$  of the form*

$$G + \sum_H \alpha_H H, \quad \alpha_H \in \mathbb{Z},$$

*the sum taken over those subgroups  $H$  of  $G$  for which  $H/O_l(H)$  is quasi-elementary. Here  $O_l(H)$  is the  $l$ -core of  $H$  (the largest normal  $l$ -subgroup).*

*Sketch of the proof.* This is shown in the course of the proof of [7, Theorem 5.6.11], but since the actual statement of the theorem is somewhat weaker, we summarise for the benefit of the reader the main ideas of the proof. It is enough to prove that for any prime number  $q$ , there exists a  $\mathbb{Z}_l$ -isomorphism in  $G$  of the form

$$aG + \sum_H \alpha_H H,$$

where the sum is over subgroups  $H$  for which  $H/O_l(H)$  is quasi-elementary,  $\alpha_H \in \mathbb{Z}$ , and  $a \in \mathbb{Z}$  is not divisible by  $q$ . In other words, it is enough to exhibit suitable elements of  $B(G) \otimes \mathbb{Z}_{(q)}$  that become trivial under the natural map  $B(G) \otimes \mathbb{Z}_{(q)} \rightarrow R_{\mathbb{F}_l}(G) \otimes \mathbb{Z}_{(q)}$ . To do that, one first writes  $\mathbf{1} \in B(G) \otimes \mathbb{Z}_{(q)}$  as a sum of primitive idempotents  $\mathbf{1} = \sum_H e_H$ , which are described in [7, Corollary 5.4.8], with property that each  $e_H$  is induced from  $B(H) \otimes \mathbb{Z}_{(q)}$  ([7, Theorem 5.4.10]). One then shows that under the map

$$B(G) \otimes \mathbb{Z}_{(q)} \longrightarrow R_{\mathbb{F}_l}(G) \otimes \mathbb{Z}_{(q)},$$

only those  $e_H$  map to non-zero idempotents, for which  $H/O_l(H)$  is  $q$ -quasi-elementary. Since each  $e_H$  is a linear combination of  $G$ -sets  $G/U$ ,  $U \leq H$ , with coefficients whose denominators are not divisible by  $q$ , the result follows.  $\square$

**Corollary 9.5.** *Let  $G$  be a finite group and  $l$  a prime number. Any Brauer relation can be written as a sum of relations induced from soluble subgroups of  $G$  and a  $\mathbb{Z}_l$ -isomorphism.*

*Proof.* Let  $\Theta$  be an arbitrary Brauer relation in  $G$ , let  $R = \mathbf{1}_G + \sum_H \alpha_H H$  be a  $\mathbb{Z}_l$ -isomorphism, as given by Theorem 9.4. In particular, all subgroups  $H$  in the sum are soluble. Since the subgroup of  $B(G)$  that consists of  $\mathbb{Z}_l$ -isomorphisms forms an ideal in  $B(G)$ , we see that

$$\Theta \cdot R = \Theta + \sum_H \alpha_H \operatorname{Ind}^G \operatorname{Res}_H \Theta$$

is a  $\mathbb{Z}_l$ -isomorphism, and the claim is established.  $\square$

*Proof of Theorem 9.1.* It is easy to see that if  $R$  is a  $\mathbb{Z}_l$ -isomorphism, then  $\operatorname{ord}_l(C_R(\mathbf{1})) = 0$  (and in fact, the same is true with  $\mathbf{1}$  replaced by any finitely generated  $\mathbb{Z}[G]$ -module). Thus, Corollary 9.5 reduces the proof of the theorem to the case that  $G$  is soluble.

Writing  $\Theta$  as a sum of primitive relations listed in Theorem A, we see immediately by inspection that the relations  $\Theta'$  that generate  $\operatorname{Prim}(G)$  in the cases 1, 2, and 4 satisfy  $C_{\Theta'}(\mathbf{1}) = 1$ . The remaining assertions of the theorem follow from a direct calculation for the generators of  $\operatorname{Prim}(G)$  in the case 3.  $\square$

## REFERENCES

- [1] M. F. Atiyah, C. T. C. Wall, Cohomology of groups, in J.W.S. Cassels, A. Fröhlich (Eds), Algebraic Number Theory, Academic Press, 1967.
- [2] A. Bartel, Large Selmer groups over number fields, Math. Proc. Cambridge Philos. Soc. 148 (2010), 73–86.
- [3] A. Bartel, On Brauer-Kuroda type relations of S-class numbers in dihedral extensions, J. reine angew. Math. 668 (2012), 211–244.
- [4] A. Bartel, Elliptic curves with  $p$ -Selmer growth for all  $p$ , Q. J. Math. (to appear), arXiv:1204.1166 [math.NT], 2012.
- [5] A. Bartel, T. Dokchitser, Brauer relations in finite groups II — quasi-elementary groups of order  $p^a q$ , arXiv:1110.6618, 2011.
- [6] A. Bartel, B. de Smit, Index formulae for integral Galois modules, arXiv:1105.3876 [math.NT], 2011.
- [7] D. J. Benson, Representations and Cohomology I, Cambridge University Press, 1991.
- [8] G. Berz, Permutationsbasen für endliche Gruppen, Ph.D. thesis, Augsburg, 1994 (Zbl 0924.20003).
- [9] W. Bley, R. Boltje, Cohomological Mackey functors in number theory, J. of Number Theory 105 (2004), 1–37.
- [10] R. Brauer, Beziehungen zwischen Klassenzahlen von Teilkörpern eines galoisschen Körpers, Math. Nachr. 4 (1951), 158–174.
- [11] S. Bouc, The Dade group of a  $p$ -group, Invent. Math. 164 no. 1 (2006), 189–231.
- [12] D. Burns, On Artin formalism for the conjecture of Bloch and Kato, Math. Res. Lett. (to appear).
- [13] P. Deligne. Les constantes des équations fonctionnelles des fonctions  $L$ , In Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., Vol. 349. (1973) Springer, Berlin, 501–597.
- [14] T. Dokchitser, Solomon’s induction in quasi-elementary groups, J. Group Theory 14 (2011), 49–51.
- [15] T. Dokchitser, V. Dokchitser, Regulator constants and the parity conjecture, Invent. Math. 178 no. 1 (2009), 23–71.
- [16] T. Dokchitser, V. Dokchitser, On the Birch-Swinnerton-Dyer quotients modulo squares, Annals of Math. 172 no. 1 (2010), 567–596.
- [17] T. Dokchitser, V. Dokchitser, Root numbers and parity of ranks of elliptic curves, J. Reine Angew. Math. 658 (2011), 39–64.

- [18] W. M. Dress, D. R. Kletzing, On prime ideals in representation rings, *Math. Z.* 133 (1973), 285–300.
- [19] W. Feit, *Characters of Finite Groups*, W. A. Benjamin New York, 1967.
- [20] W. Gorenstein, *Finite Groups*, Chelsea, 1968.
- [21] M. Herzog, Counting group elements of order  $p$  modulo  $p^2$ , *Proceedings of the AMS* 66 no. 2 (1977), 247–250.
- [22] I. Hambleton, L. R. Taylor, Rational permutation modules for finite groups, *Math. Z.* 231 (1999), 707–726.
- [23] E. B. Kahn, The relative Burnside kernel — the elementary abelian case, preprint, arXiv:0809.1450v1 [math.AT], 2008.
- [24] S. Kuroda, Über die Klassenzahlen algebraischer Zahlkörper, *Nagoya Math. J.* 1 (1950), 1–10.
- [25] R. P. Langlands, On the functional equation of the Artin  $l$ -functions, Yale University preprint, 1970.
- [26] J. Ritter, Ein Induktionssatz für rationale Charaktere von nilpotenten Gruppen, *J. Reine Angew. Math.* 254 (1972), 133–151.
- [27] G. Segal, Permutation representations of finite  $p$ -groups, *Quart. J. Math. Oxford* (2) 23 (1972), 375–381.
- [28] J.-P. Serre, *Linear Representations of Finite Groups*, GTM 42, Springer-Verlag 1977.
- [29] B. de Smit, Brauer-Kuroda relations for  $S$ -class numbers, *Acta Arith.* 98 no. 2 (2001), 133–146.
- [30] V. Snaith, Explicit Brauer induction, *Invent. Math.* 94 (1988), 455–478.
- [31] J. Tornehave, Relations among permutation representations of  $p$ -groups, preprint, 1984.
- [32] C. D. Walter, Kuroda’s class number relation, *Acta Arith.* 35 (1979), 41–51.